ÁROP – 2.2.21 Tudásalapú közszolgálati előmenetel

Biztonság támogatása

Som Zoltán

Nemzeti Közszolgálati Egyetem

Budapest, 2014

Tartalomjegyzék

Mottó:

„Az egyetértés - minden. A közvélemény támogatásával minden sikerül. Nélküle semmi."[1]

Előszó

Az információ és elektronikus információbiztonsági, védelmi és informatikai szabályok és szabályzatok (továbbiakban összességében szabályzat[2]) egyszerre kell, hogy támogassák a szervezet célkitűzéseit, a menedzsmentet ezen célok elérésében, a megfelelő döntésekhez szükséges információ biztosításában, a döntések meghozatalában (javaslattétel formájában), valamint a munkaszervezet elemi részét, a munkavállalót is munkavégzésében. A munkaszervezet teljes vertikumára ki kell, hogy terjedjen, sőt azon túl is kell nyúlnia, a beszállítók és partnerek vonatkozásában. Komplex feladat, azonban összetettségét nem az említett széles spektrumú megfelelőség alkotja, hanem a szervezeti célok elérésének támogatásában való megfelelés. Egy ilyen szabályozási keretrendszer feladata tehát elsősorban a szervezet támogatása a célok elérésében. Az elektronikus információbiztonsági[3] vezető elsődleges feladata a menedzsment kiszolgálása és a megfelelő információkkal való ellátása a döntéshozatal elősegítése érdekében. Innen származtatható minden további szerepkör, szabályzat és teendő.

Mivel végső soron minden információs rendszerben jelen van a humán faktor, az ember, így a szabályzat célja nem lehet más, mint a humán faktor támogatása és a támogatásának megszerzése oly módon, hogy a folyamat aktív és támogató részese legyen. Azt kell, hogy érezze minden egyes munkavállaló, hogy az eljárásrendek az ő munkáját segítik. Ezen koncepció és az idézet megértése nélkül kevés esély van egy jól és hatékonyan működő információbiztonsági program működtetésére. A humán faktor kapcsán be kell látni, hogy minden egyes munkavállaló egyéni, önálló individuummal rendelkezik. Azaz nem csak munkavállaló, hanem szülő, testvér, gyermek, akinek a szervezeten kívül is saját digitális élete és digitális lábnyoma van. Az az úgynevezett adattest folyamatosan növekszik életünk

[1] Abraham Lincoln

[2] A magyar nyelvben számos rokon értelműnek tűnő kifejezés létezik, amelyek azonban ha nem is élesen, de részben elkülönülnek, részben pedig a hétköznapok során nem biztos, hogy a szabályzatokban érdemes külön kezelni. Gyakorlatilag a szabályozásban sokkal inkább az információbiztonságé a kulcsszerep, és az információ bizonyos, adott reprezentálódására lehet pontosabb eljárásrendet, támogatási ajánlást definiálni.

[3] A megfogalmazás akár pontatlannak is tekinthető, hiszen az elektronikus információbiztonságról beszélünk. A 2013. évi L. törvény is így fogalmazza meg, de valójában pontosabb lehet az az elektronikus előtag nélküli használat.

során. Ha az információbiztonsági keretrendszer és program képes komplexen támogatni a munkaszervezetet, akkor ki kell terjednie a munkavállaló munkahelyen kívüli élethelyzeteire is, a tudatossági oktatásokon sort kell keríteni minden felmerülő, nem csak munkahelyi információ és informatikai biztonsági kérdés megválaszolására is.

Jelen tananyag a vezetőség, a menedzsment, a munkaszervezet céljainak elérésre tett erőfeszítéseit világítja meg az összes, szorosan kapcsolódó kérdést az információbiztonsági keretrendszer és a vezető általi támogatásán keresztül. Ennek megfelelően bizonyos részek csak érintőlegesen, utalás jellegűen kerülnek kifejtésre.

1. Bevezetés

A könyv célkitűzése, hogy valódi segítség legyen az információbiztonsági vezető kezében, így ahol csak lehetőség adódik, példákkal is illusztrálja az adott szabály, eljárás bevezetési gyakorlatát, a lehetőségekre és csapdákra egyaránt rámutatva.[4]

Jelen könyv a „Stratégia és szervezettámogatás - Rendszerirányítási szakismeretek" tanulmányi területen belül a „Biztonság támogatása" kérdéskörét kívánja minél jobban megvilágítani. Mivel az információbiztonsági keretrendszernek a „biztonság támogatása" egy, talán az egész programhoz viszonyítva vékony, de ugyanakkor kiemelten fontos szelete, így ennek megfelelően bizonyos részeket csak érintőlegesen, mintegy említés szintjén kezel a könyv. Ahol csak lehetőség van, egyszerű példákon keresztül mutatja be, hogyan alkalmazható egy-egy eljárás a gyakorlatban. Fel kell hívni azonban a figyelmet arra, hogy az információbiztonsági keretrendszer, annak programszintű implementálása munkaszervezetenként eltérő lehet, számos tényező befolyásolja. Pont ezekből a helyi, adott munkaszervezetre jellemző eltérésekből azonban akár az is következhet, hogy ami nem működött 99 helyen, az a 100. munkaszervezetben beválik. Tehát, bár az információ biztonsági, irányítási keretrendszer jelentős mankót ad az információbiztonsági vezető kezébe, a megvalósítást, annak kommunikációját, magát a programot mégis önállóan kell az adott munkaszervezetben sikerre juttatni, a helyi körülményekre implementálni.

Egyes szakemberek véleménye szerint az egyik legtöbb konfrontációval járó feladatkört vállalja magára az információbiztonsági vezető. A vezetőség, a menedzsment alapvetően költségtényezőt lát a biztonsági programban, amire költeni kell, ugyanakkor szigorúan véve nem termel közvetlen nyereséget, nehezen mérhető az ebből származó bevétel. A bevétel a káresemények elkerülésében mutatkozik meg. Az IT, vagy üzemeltetés gyakran csak a szabályokat látja benne, azaz „megmondja valaki" mit és hogyan csináljanak. A felhasználók, beszállítók, partnerek pedig azt látják, hogy már megint van egy újabb szabályzat. Az információbiztonsági vezető[5] feladata ezen gondolatok és érzelmek

[4] Fontos azonban megjegyezni, hogy minden munkaszervezet eltérő. Így a biztonsági program tényleges implementálására vagy a tudatossági oktatás menetére esetenként teljesen eltérő módszerek is működőképesek, hatékonyak lehetnek.

[5] Az információbiztonsági vezetőre számos hasonló kifejezés létezik a magyar és nemzetközi szakirodalomban is. Az információbiztonsági menedzser, CISO: ChiefInformationSecurityOfficer. Melyek mind picit mást jelentenek, de ezen különbségek részletezésére nem térek ki, jelen tananyagban ekvivalens módon kezelem.

valósághoz való közelítése. Tehát míg a menedzsmentet jellemzően az üzleti célok és előnyök valamint a kockázati faktor győzi meg, addig a felhasználókat esetében komoly szerepe lehet az érzelmeknek és annak, hogy a munkafolyamatokban értéket legyen képes teremteni a program. A program végrehajtásának sikerességében, a támogatottság megszerzésében pedig minden érintettel[6] fel kell venni a kapcsolatot és ezt követően meg kell tudni mutatni, hogy az információbiztonsági program hogyan járul hozzá, az adott személy munkájához, hogyan teremt értéket, munkavállalótól indulva a teljes munkaszervezet egészére vonatkoztatva.

[6] Az informatikai üzemeltetés lehetséges előnyeihez ad támpontot az 1. ábrán látható ITIL folyamatok integrálása, amely kevesebb felhasználói interakciót, szabályozottabb folyamatokat jelenthet.

2. Kockázat feljegyzési követelmények

Mottó:
„A mérés kulcsfontosságú. Ha nem tudunk valamit mérni, akkor nem tudjuk irányítani.” [7]

2.1. Értelmezés

A kockázat feljegyzési követelmények logikailag az információbiztonsági kockázatmenedzsment és megfelelés részen belül helyezhetők el.[8] Céljuk az, hogy az információbiztonsági menedzser, vezető biztosítsa és megalapozza a folyamatokat és sztenderdeket az információ veszélyeztetettségi állapot jelentésekhez, továbbá megvalósuljon az irányítás mind normál, mind pedig eseményvezérelt helyzetben. Nagyon sok tényező határozza meg, hogy mit, kinek és mikor kell jelentenie. Ezek a tényezők függnek:

- a szervezet típusától,
- a szervezeti kultúrától,
- az elfogadható biztonsági szinttől (azaz a szervezet által elfogadott biztonsági kockázattól és étvágytól),
- a biztonsági szint toleranciájától,
- a helyi és vonatkozó szabályozástól, jogszabályoktól,
- az esemény súlyosságától, valószínűségétől és a lehetséges fenyegetettség következményeitől,
- egyéb iparági, szervezeti sajátosságoktól.

A többféle nézőpont és kritérium vonatkozásában is igaz, hogy a menedzsment által definiáltnak és jóváhagyottnak kell lennie a kockázat jelentési kötelezettségnek, a szabályozásnak. A jelentési folyamatnak és struktúrának tartalmaznia kell azt az eljárásrendet, amely biztosítja, hogy szabálykövető módon annak minden fontos részlete, típusa, a változás természete jelentésre kerül. A szabályozott jelentéstételi kötelezettség

[7]Robert S. Kaplan, David P. Norton

egyrészt azt a célt szolgálja, hogy kommunikálja a kockázat státuszát, állapotát. Másrészt emlékeztet arra, hogy a felelősség kollektív felelősséget[9] jelent a kockázatkezelésben, az egész szervezet számára.

2.2. Alapvető elvárások és koncepciók

Elvárás a követelmények megfogalmazása a kockázat rendszeres és szabályozott jelentéséhez, a kockázat kommunikációjához, a tudatossági képzéshez és konzultációhoz. A szervezet teljes egészére igaz kell, hogy legyen a személyes felelősségvállalás, az egyenszilárdság megteremtése érdekében. Elvárás továbbá a kockázat monitoring és jelentős kockázati fenyegetettség változás esetén a kommunikációs jelentés is, ezeken kívül pedig valamilyen rendszeres jelentés abban az esetben is, ha nincs (vagy nem érzékeltük, nem jelentettek) változás. Az események típusa lehet olyan, amiket jelentenek és olyan, amik eszkalálódhatnak. A jelentések tartalma a szervezet többféle szintjéről érkezhet és azok címzettjei is többfélék lehetnek. Nem feltétlenül következik, hogy a jelentéseknek mindig az információbiztonsági vezető a címzettje, hiszen lehet egy ilyen információáramlásban feladó, címzett, érintett, informált vagy tájékoztatott.

A RACI[10] modell 4 kategóriát határoz meg: 1) R: responsible, azaz ki a felelős az adott feladat végrehajtásáért, ki végzi el a feladatot, 2) A: accountable, azaz ki az, aki elszámoltatható azért, hogy a munka el legyen végezve.[11] 3) C: consulted, azaz konzultáló, be kell vonni, egyeztetni kell vele, kétirányú kommunikáció kell, hogy megvalósuljon, de nem az övé a döntés. 4) I: informed, azaz informálandó az adott személy a feladat elvégzése során, vagy azt követően, egyirányú kommunikációval. A modell kiegészülhet az S: support, azaz a felelős munkáját segítő személlyel és az O: out of theloop, azaz kihagyandó személyek definiálásával is. A kockázat feljegyzésnél a fentiekben jól körül lettek határolva a feladatok, a kulcs kockázati tényezők feltérképezése és monitoringja, amely egyrészt periodikusan, másrészt változás esetén is meg kell, hogy történjen.[12]

[9] Nem lehet más a cél, mint az egyenszilárdság megvalósulása, ehhez minden egyes munkavállalónak tudnia kell, hogy a biztonság, rajta is múlik.

[10] Felelősség hozzárendelési mátrix. A feladatok, felelősségek nyomon követésére szolgál. Nevét a négy általa meghatározott kategóriából kapta: Responsible, Accountable, Consulted, Informed.

[11] Egy feladatnál egy elszámoltatható lehet.

[12] Ezt követően természetesen további teendők is vannak, hiszen a kockázatkezelést a megváltozott feltételekre is végre kell hajtani.

RACI táblázat																										
A fő irányítási gyakorlatok	Vezetői testület	Ügyvezető	Pénzügyi vezető	Operatív vezető	Üzleti vezetők	Üzleti folyamatok tulajdonosai	Stratégiai végrehajtó bizottság	Projekteket vezető irányító bizottság	Project menedzsement iroda	Értékek kezelési irodája	Vezető kockázatkezelési tisztviselő	Információbiztonsági vezető	Arhitektúra bizottság	Vállalati (egységes - központi) kockázatkezelési bizottság	A Humánerőforrás vezetője	Megfelelőség	Audit	Informatikai vezető	Az architect egység vezetője	A fejlesztési egység vezetője	Az IT műveletek vezetője	Az IT adminisztráció (ügykezelés) vezetője	Szolgáltatás menedzser	Információ biztonsági menedzser	Üzletmenet folytonossági menedzser	Adatvédelmi felelős
Azonosítani és értékelni a beszállítói kapcsolatok és szerződéseket.			C			C									C	C	C	A	C	C	C	R	C	C	C	
A beszállítók kiválasztása.			C			C									C	C	C	A	C	C	C	R	C	C	C	
A beszállítókkal való kapcsolatok és szerződések menedzselése.						I									C	C	C	A	C	R	R	R	C	C	C	
A beszállítói kockázatok menedzselése.						C					R				C	C	C	A	C	R	R		C	C	C	C
A beszállítói teljesítmény és megfelelés monitoringja.			I			C					C				C	C	C	A	C	R	R		C	C	C	C

2. ábra: RACI tábla (COBIT 5, Enabling processes chapter)

2.3. Áttekintés

Mottó:
„BIZTONSÁG: Olyan kedvező állapot, amelynek megváltozása nem valószínű, de nem is kizárt.”[13]

2.4. A hatékony információbiztonsági program menedzselés a feljegyzési követelmények tükrében

Vizsgáljuk meg alaposan a „kockázat feljegyzési követelmények”-et, jelen esetben szavanként! A kockázatot általában valamilyen változás tükrében tudjuk értelmezni. Ennek kezelésére vonatkozó törekvésünk, hogy annak elkerülésére, kezelésére eljárásrendet készítünk. Ezt a dokumentációs lépést hívhatjuk feljegyzésnek. Egy dokumentum maga képes előírni valamilyen kötelezettséget, tevékenységet, például a megelőzéshez szükségeset. A feljegyzés pedig, bár erősen rokon értelmű, mégis inkább valamilyen eseményt, történést rögzít. A gyakorlatban nem könnyű elhatárolni a dokumentumokat a feljegyzésektől, azok keveredhetnek is. Tehát míg a dokumentálást inkább abban az értelemben használjuk, hogy

[13]Vasvári György, 1997

ellenőrizhetővé, nyomon követhetővé és visszakereshetővé tegye a működést, addig a feljegyzési követelményt inkább abban az értelemben használjuk, hogy feljegyzésre kerül a tapasztalt nem megfelelőség, vagy audit-eltérés. A feljegyzés tehát egy olyan dokumentum, amely rögzíti az adott helyzetet, tevékenységet, például a döntések háttér információit.

A kockázatkezelés olyan alapvetés, amelynek minden folyamatba be kell épülnie. Ennek oka, hogy számtalan változás éri a szervezetet és annak külső - belső folyamatait.[14] Előfordulhat, hogy ezek kismértékben befolyásolják a kockázatokat, de kulcselemeket is érinthetnek. Egy változásnak sokféle vonzata lehet, ez csak akkor derül ki, ha minden tényező, minden függőség tételesen megvizsgálásra kerül. Ennek kezelésére egy munkaszervezeten belül szolgálhat az elektronikus vagy papír alapú változáskezelő lap, vagy feljegyzési napló. A megnevezése eltérhet, de célját tekintve a fókusz azon van, hogy ha bármi (ha a legkisebb dolog is) megváltozik, akkor arról feljegyzés, dokumentum készüljön. Ez alapján pedig az érintett területek képviselőivel, a függőségi mátrix figyelembevételével értékelni kell a kockázatokat, annak változását. Az értékelést, a kezelésre hozott intézkedéseket (vagy annak hiányát) pedig szintén dokumentálni szükséges, hogy utólag is visszakereshető legyen, transzparens módon láthatóvá téve a változás, a megbeszélés és az (esetleges) intézkedések lényeges pontjait.

Ebből jól látható, hogy a kockázatok kezelésére vonatkozó eljárás, a biztonsági szint fenntartása, az ezeket a feljegyzési követelményeken keresztül érkező, elsődleges impulzusok kezelése nem egyetlen ember feladata a munkaszervezetben. Ezen feljegyzések elkészítése, az elsődleges bejelentés megtétele mindig az adott munkafolyamatban résztvevő munkavállaló vagy csoport feladata. Továbbá a feljegyzések megbeszélése és abból fakadó döntések meghozatala is több résztvevős munka, a biztonság, a szakma, a vezetőség[15] együttes feladata. Ennek gyakorlati lebonyolítása a munkaszervezeti szokások függvényében eltérő lehet, azaz lehet ez egy 3 fős és tíz perces megbeszélés, amely javaslattevéssel és dokumentálással zárul, de ennél hosszabb és több résztvevős is lehet. A szervezet működési folyamataiban definiált feladatok és felelősségi körök alapján jól körülhatárolt módon meg kell, hogy legyen szabva a változások kezelése. A változáskezelési folyamat része, hogy a változásbejelentő lap az adott munkakörhöz, felelősségi körhöz kapcsolódóan feladatot határoz meg. Ennek megléte vagy elmulasztása egyaránt visszakereshető kell, hogy legyen.

[14] Azt az ideális állapotot feltételezve, hogy a szervezeti célok, üzleti elvárások jól definiáltak, abban az esetben is.

[15] : Risk, - Security, - Management - committee

Kockázatkezelés nélkül nincs jól működő biztonsági program, ez részét kell, hogy képezze a folyamatoknak.

A változáskezelés kapcsán fontos megjegyezni, hogy dokumentumtípusokhoz, eljárásokhoz, szerződéstípusokhoz egyaránt meg kell határozni a felülvizsgálati időket. Ennek egyik szerepe a változás vizsgálat, azaz történt-e esetleg változás, amely elkerülte a folyamatgazda figyelmét vagy olyan területre esett a változás, amely nem volt megfelelően lefedve, vagy definiálva. Jellemzően a folyamatokat általánosan évente érdemes felülvizsgálni, de ez erősen típusfüggő, lehet ennél rövidebb időnként is, főleg ha kulcsfolyamatról van szó; ennél nagyobb intervallumot nem javasolt meghatározni. A folyamat kockázatkezelési szempontból akkor számít jól (erősen) definiáltnak, ha változáskor valóban automatikusan elindul a kockázatkezelési ág, e nélkül nehéz reagálni a változásokra, amely biztonsági kockázatként fog jelentkezni egy vagy több folyamatban. [16] Általánosságban elmondható, hogy minden egyes változásról értesíteni kell a megfelelő szintet és személyt, hiszen csak akkor tud rá reagálni, ha tud a változásról.

Az előbbiek tükrében jól látható, hogy a biztonság nem egyszemélyes feladat és az is kitűnik, hogy a fenntartásához jól definiált folyamatok és egységes, tudatos munkavégzés szükséges. A feljegyzési, változásbejelentési dokumentumok feladója és címzettje ugyanis roppant változatos lehet egy munkaszervezetben. Elképzelhetőek olyan folyamatok, amelyekben elsődlegesen nem szerepel az információbiztonsági vezető címzettként, vagy csak, mint informálisan tájékoztatott személy van feltüntetve.

[16] COBIT 5, Enabling Processes, APO10 section részben bővebben lehet a témáról olvasni.

3. Elégedettség riport követelmények

Az információbiztonsági vezető elé kerülő kihívások[17] jellemzően abból származnak, hogy meg kell tudnia mutatni, hogy a költség és megtérülés hogyan támogatja az üzleti folyamatokat valamilyen biztonsági intézkedés vonatkozásában. Az alábbiakban így inkább tipikus buktatókra kívánjuk felhívni a figyelmet. Jellemzően azok az incidensek, amelyeknek valamilyen érzékelhető kihatása van a szervezetre, kerülnek inkább a vizsgálódás középpontjába, ritkán esik szó sikeresen elhárított támadásról.

3.1. Értelmezés

Az elégedettségi riport követelmények, kockázatkezelési problémák és változáskezelés rész csoportosítását tekintve az információs kockázat menedzsment és megfelelőség részbe tartozik.[18] Általánosan jellemző, hogy a szervezeteknek meg kell felelniük működésük során többféle külső és belső, jogi és szabályozási követelményeknek. Az információbiztonsági menedzser felelőssége, hogy olyan tervet készítsen, amely révén a szervezet a lehető legnagyobb mértékben megfelel a szabályozási környezetnek, figyelembe véve a szervezet erőforrásait és egyéb, a szervezetre jellemző paramétereket. Ezen terv mérföldkövekre, állomásokra bontható, amelyek mentén történő előrehaladásról[19] tájékoztatást kell nyújtani, konzultálni szükséges a felső vezetéssel és egyben érdemes is promóciós, kommunikációs lehetőségként az előrehaladásokat propagálni. Maga a szabályozási környezetnek való megfelelés mértéke is kockázati tényező. Általánosságban igaz, hogy nem hatásos rövid idő alatt túl nagy változásokat foganatosítani a szervezetben. Alapvető követelmény kell, hogy legyen az összes üzleti és informatikai folyamatban a teljes életciklusra vonatkoztatva a változás kezelése. Nagyon egyszerű példával élve mégis érzékeltetni lehet a különbséget a között, hogy ha a megvalósíthatósági, tervezési, kivitelezési fázisban megtörténik a kockázatok elemzése, értékelése, a folyamatokba az ellenőrzési pontok beépítése és a között az állapot között, amikor megtörténik valamilyen rendszer vagy szoftver leszállítása, amelyről nincs információ, így nem csak

[17] Ahogy a fentiekben is többször történt rá utalás az információbiztonsági vezető élete nem feltétlenül könnyű, de tele van szép kihívásokkal.

[18] Information Security Governance, Information Risk Management and Compliance, Information Security Program Development and Management, InformaionSecurity Incident Management (ISACA, CISM 2013)

[19] A folyamatos és rendszeres, de ugyanakkor rövid tájékoztatás több irányban is meg kell, hogy valósuljon a program promótálása érdekében.

információbiztonsági, informatikai, hanem üzletmenet folytonosság szempontjából is kritikus. Van néhány folyamat, ami az elsődleges folyamatok közé tartozik, mint például a kockázatkezelés, a változáskezelés, frissítés, minőségbiztosítás és nem utolsó sorban az elfogadás felhasználói tesztelése. Az információbiztonsági vezetőnek tudnia kell ezen folyamatokról, tudnia kell azonosítani a kockázatokat a különböző életszakaszokban, továbbá tisztában kell, hogy legyen (a folyamatokba épített ellenőrzőpontokon keresztül) azokkal a folyamatokkal, eljárásokkal, gyakorlatokkal, amelyeken keresztül rálátása nyílik arra, hogy az egyes egységek hogyan értékelik a saját területükön felmerülő kockázatokat. Ezen felmérés alapján kell tudnia meghatározni a megfelelő eszközök kiválasztását a kockázatok kezelésére esetleg többféle alternatíva kidolgozásával, majd a vezetőség döntését követően végrehajtani a kockázatok csökkentésére irányuló, jóváhagyott lépéseket. Például kiválasztásra kerül egy új csomagszűrő alkalmazás, az egyszerűség kedvéért legyen tűzfal, amelyet az üzemeltetés választ ki és ennek üzembeállításáról csak akkor értesülnek az érintettek, amikor az átállás miatti kiesésről értesítés érkezik. Az első és legnagyobb probléma bármilyen szolgáltatásnál az szokott lenni, hogy a szóbeli ígéretek és a szerződés között nem teljes az összhang. Gyakran a pénzügyi teljesítést követően csökken a support és tanácsadás intenzitása. Nem egyértelmű, hogy a régi szabályrendszert ki és mikor fogja beállítani (migrálni) a már működő új eszközön, annak garanciaidőn belüli meghibásodása esetén milyen eljárásrend és milyen határidők lépnek életbe. Elvonatkoztatva a tűzfaltól, szó lehet bármilyen más hardverről, alkalmazásról, eljárásrendről, igénybe vett szolgáltatáscsomagról. Az információbiztonsági vezető feladata, hogy ezeket az összes érintett jogi, költségvetési, stb., érintett osztályokkal, vezetőkkel egyeztesse a kockázati szempontok kiértékelése érdekében,valamint számunkra olyan támogatást tudjon biztosítani, amely a pontoson specifikált szerződéses pontok következtében csökkenti a kockázatokat, szabályozottá teszi a folyamatokat, ellenőrzési lehetőségeket, pontokat iktat be.

3.2. Alapvető elvárások és koncepciók

Az alapelvek és a gyakorlatok összhangba hozásához az információbiztonsági vezetőnek tisztában kell lennie azzal, hogy mi történik a szervezetben, a szervezeti folyamatokban. Ezt legjobban a folyamatokba beépített kontroll vagy ellenőrzési pontokon keresztül lehet megvalósítani. Ezen metodikának, a kockázatkezelésnek a teljes életciklusban meg kell valósulnia, az alapelvekben és a gyakorlatban is. Tisztában kell lenni azzal, hogy a

változás (hardver, szoftver, folyamatok, patch, frissítések, jogszabályi környezet, stb.) hogyan érinti a kockázatkezelési tervet, a folyamat része kell, hogy legyen a kockázatértékelés elvégzése is.

3.3. Áttekintés

Mivel a fentiekben elég sok szó esett már a kockázatkezelésről, így ebben a részben a hangsúlyt inkább a változáskezelésen keresztüli megvilágítás, valamint a sikeres kockázatcsökkentéshez szükséges tényezők áttekintése kapja, kitérve néhány jellemző, gyakran felmerülő nehézségre.

3.3.1. Kommunikációs hibalehetőségek

A kockázatkezelési program sikeres kivitelezéséhez először is egy jóváhagyott program szükséges. Azonban tegyük fel a kérdést, mi szükséges ahhoz, hogy legyen egy jóváhagyott program? Az információbiztonsági vezető a szervezet alapállapotának lemérését követően javaslatot tesz, de mi kell ahhoz, hogy ez a javaslat elfogadásra kerüljön? Ez a lépés kulcsfontosságú a későbbi sikeres program szempontjából. Olyan program szükséges, amely előadását, voltaképpen eladását követően, elkötelezett támogatásra talál a felső vezetés részéről. Próbáljuk meg áttekinteni mit érdemes kerülni a program ismertetésekor! [20]

3.3.1.1. Szóhasználat

Kerüljük a túlzott technológiai és szakmai szóhasználatot! Szakmabeliekkel folytatott beszélgetésben fontos lehet, hogy milyen firmware és hardver verziókkal rendelkezünk és ezek melyik sebezhetőségét milyen portokon keresztül próbálják meg kihasználni, de itt sokkal inkább eladásról[21] van szó. Tehát el kell tudni adni a programot, méghozzá érthetően. A vezetésnek, a döntése meghozatalakor tisztában kell lenni azzal, hogy X befektetett forint

[20] A program és stratégia, ahogy arra már kitértem jelen esetben rokon értelmű szavakként vannak kezelve. A megállapításaim érvényesek mindkettő „eladására” vonatkozólag.
[21] A biztonsági program, az amit természetesen alternatívák felkínálásával „értékesíteni” kíván a biztonsági vezető.

esetén Y helyreállítási költség spórolható meg esetlegesen. Ki kell tudni mutatni X és Y viszonyát.

3.3.1.2. A másik fél megértésére törekvés

Meg kell érteni a felső vezetés álláspontját a biztonsággal kapcsolatban. A felső vezetés véleménye ugyanis kiáramlik a teljes szervezetre. Amennyiben jelenleg hiányzik a (teljes) támogatás, akkor meg kell vizsgálni, hogy mi okozza ezt! Lehet, hogy több időt kell szánni a kockázatok érthető és pontos bemutatására, még a program eladása, bemutatása előtt. Mintegy felkészítve, ráhangolva a döntéshozókat.[22] Esetleg más, üzleti szempontból, üzleti szóhasználatot követve kell a szükséges fogalmakat bemutatni, megfelelő vizualizációt alkalmazni.

3.3.1.3. Ki kell emelni az üzleti kockázatokat

Ez azt is jelenti, hogy rangsorolni kell az eladni kívánt terméket, csak a legfontosabb, legsürgetőbb kérdések kiemelése is lehet egyfajta politika a figyelem megragadására. És bár a figyelem felkeltésére a legjobb módszer, ha valamilyen esemény van, de mégis azt kell tudni bemutatni, hogy milyen előnyökkel jár, ha nem esemény-orientáltan működik a biztonsági program. Ha valamilyen esemény nem fog előfordulni (vagy csökken előfordulásának a valószínűsége) akkor az milyen üzleti hatásokat, költségmegtakarítást jelenthet. A bemutatás során érdemes a speciális szakszavak kerülése, fontos megfogalmazni a támogatásra igényelt (költség) keretet is. Továbbá vegyük figyelembe, hogy bármilyen kiváló is a prezentáció és az előadott megoldás, csak limitált idő és egyéb forrás áll rendelkezésünkre.

3.3.1.4. Megjelenés

Az interneten található egy csoportkép, hozzávetőleg 15-20 ember van rajta és felette egy kérdés: Ki a vezető a képen? A válasz nem volt megadva, költői kérdés volt, a fényképen mindenki elegáns ruhát visel, de csak egyetlen személyen volt nyakkendő. Bizony az öltözet

[22] A szervezet felmérése folyamán érdemes részleges eredményeket, információkat adni már az egyes információblokkok kiértékelésekor. Például adott osztály, adott komponens vonatkozásában; a végén természetesen a záró értékelést követheti a javasolt alternatívák bemutatása.

kiemelkedően fontos, amikor értékesíteni szándékozunk valamit. Az értékesítés szempontjából számít az összhatás és ebbe beletartozik a megjelenés, az öltözet is. Ebben az esetben pedig az információbiztonsági vezető minden mozdulatával, szavával, megjelenésével, stb. hitelesen kell, hogy tudja eladni a biztonsági stratégiát. Öltözetünk alkalmazkodjon a felső vezetés ruházkodási szokásaihoz!

3.3.1.5. Légy tájékozott!

„Csináld meg a házi feladatot más szervezeteknél!" Értékes információ lehet, hogy más szervezeteknél mi a helyzet, ott hogy oldják meg a hasonló kérdéseket.[23] Ez azért is fontos, mivel a legtöbb szervezetben korlátozottak a rendelkezésre álló erőforrások (idő, emberek, pénz),ezért annak pszichológiai hatása is van, hogy ha máshol már valamilyen módszert alkalmaznak és bevált. Meg kell tudni mutatni a biztonság értékteremtő erejét, ami lehetővé teszi, hogy mindenki tegye a dolgát, az egész szervezet a szervezeti célokért (kiesésmentesen) tudjon dolgozni. Ezeket az előnyöket meg kell tudni fogalmazni a kulcsfontosságú döntéshozók számára!

3.3.1.6. Csak a lényeget

„A kevesebb néha több" mondás érvényes a prezentációra is. A prezentáció során a közönség, vezetőség fejében felmerülő ki nem mondott kérdésekre is választ kell adni. Miért vagyok itt, Mit akarnak Tőlem, Mennyibe kerül ez? A prezentáció diái, grafikonja legyenek jól áttekinthetőek és érthetőek, minél egyszerűbb, annál jobb. Láthatóvá kell tenni, vizualizálni kell az összehasonlításokat, költségeket. Nem kell, hogy minden információt tartalmazzon, ami szükséges, ami kérdésként felmerül, az szóban is kiegészíthető. Választ kell adni azokra a kérdésekre, hogy mekkora kockázattal jár ez, mi a valószínűsége, hogy bekövetkezik, mennyibe kerül, ha megvalósul a beruházás, milyen további teendők, költségek merülnek fel? Például: kollégák oktatása, gyorsabb hardver, stb.

[23] A hasonló szervezeteknél jól működő megoldások nem jelentenek garanciát a sikerre és a működésre, de mégis olyan lehetőséget teremtenek, hogy a tapasztalatok felhasználásával már a kitaposott, kevesebb buktatót tartalmazó úton lehet haladni.

Mindezek fókuszban tartása hatékonyan támogathatja a biztonsági program elfogadását. A fentiek inkább az elkerülendő magatartásformák irányából voltak megfogalmazva, de számos további komponens van, amelyek sikertényezőnek is tekinthetőek. A felső vezetés támogatásának megszerzése hónapokig, de akár évekig is eltarthat. A jelenlegi törvényi háttér természetesen jelentősen felgyorsíthatja ezt a folyamatot. Az biztos, hogy az információbiztonsági vezető hite a programjában kiemelten fontos.

3.3.2. Kritikus sikertényezők

1. kritikus sikertényező: A vezetőség támogatásának fenntartása.

Nemzetközileg alátámasztott tény, hogy hiába léteznek jól dokumentált, részletes folyamatleírások, azok nem garantálják a sikeres csapatmunkát vagy a szervezeti sikereket. [24] Nem használhatóak, ha nincs mögötte a vezetőség támogatása, vagy fennakadást okoz a munkafolyamatokban, vagy ellenállást vált ki a munkavállalókból. Ezért is szükséges a biztonsági politika népszerűsítése, minden egyes kollégához való eljuttatása. A nagyon sikeresnek ítélt technika egy lehetséges felépítése egy-egy rövid, személyes beszélgetés minden felső és lehetőség szerint középvezetővel. A négy fő ajánlás erre vonatkozólag, fogalom szinten: 1. kivonatos (rövid), 2. egyéni, azaz személyes, 3. tervezett[25], 4. beszélgetés (kétirányú kommunikáció). Ezen találkozók célja a személyes kapcsolat megteremtése és nem csak a biztonsági elképzelések kommunikálása, hanem információszerzés annak érdekében, hogy a biztonság hogyan képes támogatni az adott szervezeti egység munkáját. Az ember természeténél fogva alapvetően segítőkész, így meg kell tudni mutatni ezen beszélgetés során, hogy pontosan miben kér segítséget. Továbbá választ kell, hogy tudjon adni arra a kérdésre is, hogy miért jó az információbiztonsági folyamatok integrálása a saját folyamataikba. Az emberek szeretik érezni, hogy munkájuk, hozzájárulásuk az egészhez fontos, így ez is lehet a hatásgyakorlás eszköze. További példák: megfelel-e az egység a törvényi és belső követelményeknek, csökkenthető-e az adatfeldolgozás, hozzáférés ideje, biztonságosabbá tehető-e a rendszer, egyszerűsíthetőek-e a folyamatok például: valamilyen tisztség alapú hozzáféréssel, így új munkavállalók hamarabb kaphatnak hozzáférést, csökkenthető-e a veszteség és az egység reputációjának megóvása mondjuk laptop titkosítással, annak

[24]Information Security Management Handbook, Sixth Edition, Harold F. Tipton and Micki Krause, 2007, Auerbach Publications, ISBN:9780849374951

[25] Tervezett, egyeztetett időpontban, megfelelően strukturált, irányított beszélgetés.

elvesztése esetén. Kommunikálni kell azon előnyöket, amiket a központi felügyelet, menedzsment biztosít a részlegnek, azzal szemben, ha az adott egység „kilóg a sorból”.

2. kritikus sikertényező: A szervezeti kultúra.

Egy munkaszervezet működése sokban hasonlít az emberi szervezet, az emberi test működéséhez. Minden része összehangoltan kell, hogy működjön annak érdekében, hogy jól funkcionáljon. És ahogy az emberi szervezetben sem lehet kiemelni egyetlen szervet, amely a test biztonságáért felel, így a munkaszervezetekben is így van ez. Tehát a biztonság nem csak az információbiztonsági vezető vagy csoport feladata. Ennek megvalósításához, illetve megvalósulásához a teljes szervezet hatékony együttműködésére szükség van. A szervezeti biztonsági kultúra alapján három jól elkülöníthető csoportra jellemző vonások állapíthatóak meg.

a, Magas: A projektekbe bevonják az információbiztonsági vezetőt is, már a kezdeteknél. Az információbiztonsági vezető beosztását tekintve magas szinten helyezkedik el a szervezeti hierarchiában. Rendszeres riport készül az aktuális helyzetről a felső vezetés számára, amely kitér a futó projektekre, változásokra, lényeges biztonságot érintő tényezőkre. Minden munkavállaló tisztában van az információbiztonság fontosságával és tudja, hogy jelenteni kell, ha incidens (vagy változás) történik. A vezetés látja, hogy a biztonsági intézkedések a szervezeti célokat szolgálják és csökkentik a kockázatokat.

b, Mérsékelt: A munkavállalók részesülnek valamilyen képzésben az információbiztonság témakörében. Bár hozzá van rendelve a feladat vagy felelősség egy munkavállalóhoz, de az valamilyen informatikai, vagy más osztályon főfeladatként más tevékenységet végez. Létezik biztonsági politika, de nem élvez széles körű támogatottságot, jellemzően az informatikai vagy jogi osztály szerkesztette meg. Az információbiztonsági intézkedések alatt jellemzően informatikai biztonsági intézkedéseket értenek a szervezetben, jelszavak, hozzáférések tekintetében és azokra korlátozva. Változások jellemzően csak reaktív módon következnek be, például audit után vagy eseményvezérelt módon.

c, Alacsony: Ha léteznek is biztonsági házirendek, azok csak feljegyzések formájában érhetőek el. A biztonság alatt a felhasználónév – jelszó párost értik, nem egyértelműen meghatározottak a feladatkörök, hogy ki felel például a vírusirtó, tűzfal, egyéb

komponensekért. A rendszerek dokumentációja hiányos, vagy nem létezik. Az információbiztonsági törekvésekre a költségvetés az informatikai költségeken belül kerül értelmezésre. Ha létezik is erre kinevezett kolléga, az csak adminisztratív célokat szolgál, nincs meg a szükséges végzettsége és a tudása.

Ezen meghatározás alapján ez a skála folytonosnak tekinthető, tehát az értékek között is számos egyéb állapot lehetséges, csupán nagyságrendi besorolás szempontjából érdemes használni. Fontosnak tartom kiemelni, hogy a szervezeti biztonsági szint nem csak költségvetés kérdése.

3. kritikus sikertényező: A biztonsági tanács megalakítása

A információbiztonsági tanács képezi a gerincét az információbiztonság szervezeti támogatásának. Egyrészt felügyeli az információbiztonsági stratégia és program végrehajtását,másrészt könnyebben és tisztábban lehet megfogalmazni azokat a szervezeti célokat, amely mögé már így nem csak egyetlen ember, hanem a tanács adja a támogatását. A tanácsnak ezen kívül meg kell fogalmazni egy olyan világos jövőképet, amelyre akár azt is mondhatjuk, hogy vízió. Ez a vízió egy olyan jövőprogram, amely mögé egyrészt fel lehet sorakozni, másrészt mégsem annyira konkrét, hogy a cselekvési teret szűkítse.

A tanácsnak lehetnek állandó és meghívott tagjai. A meghívott tagok mindig az adott szakterületet tudják képviselni, például: technikai megvalósítás, hardverek. Így a szükséges (résztvevő) részleg támogatása is jobban biztosítható. A tanács jobban tudja érvényesíteni és kommunikálni a program végrehajtásához szükséges tényezőket. Általánosan elmondható, hogy nagyobb tisztelete van egy tanácsnak, emberek közösségének, mint ha egyetlen ember képviselné az adott programot. Az egyes tanácstagok pedig a saját területükön, ahol vezetői pozícióban vannak, szintén jobban tudják kommunikálni a terveket és változásokat.

A tanács további lehetséges feladata:

- Felügyeli a biztonsági programot. Magának a tanácsnak a létrehozása is jelzi a vezetés elkötelezettségét. A tagjai a szervezet életében jelentős befolyással bíró személyek, így könnyebben fogadhatóak el a változások a folyamatokban.
- Döntés a projektek elindításáról. Minden szervezet csak korlátozott erőforrásokkal rendelkezik. Ezen erőforrásokat kell a meglévő projektek között felosztani a szervezeti célok figyelembevételével. A cél a kockázatok csökkentése, arányos

befektetések révén, valamint ésszerű ellenőrzési pontok beiktatása a folyamatokba. A tanácsnak aktív szerepe kell, hogy legyen a kezdeményezések megértésében.

- Fontossági sorrendet kell felállítani a cselekvési tervben. Ez történhet a kockázati terv alapján, azaz mi a legnagyobb rizikófaktor, mely esemény bekövetkeztekor legnagyobb a pénzügyi veszteség. Ez esetleg történhet az adott kockázat csökkentésére irányuló legkönnyebben megvalósítható tevékenység, vagy egyéb helyi szempontrendszer alapján is.
- Biztonsági szabályok ajánlása. Időszakosan és szisztematikusan felül kell vizsgálni a biztonsági szabályokat is. Ennek a felülvizsgálatnak támogatnia kell a jobb megértést, praktikus használhatóságot és a szervezeti támogatottságot is.
- A tanács tagjainak mandátumát felül kell időszakosan vizsgálni. Amikor a tanács megfogalmazza azt a víziót, amely a stratégia és program alapja lesz, akkor egy célt tűz ki. Meg kell vizsgálni, hogy a szabályzatok implementálásakor és felülvizsgálatakor mennyire teljesülnek ezen célkitűzések. Évente érdemes felülvizsgálni, hogy a kitűzött céloknak megfelelően működik-e a tanács.

4. kritikus sikertényező: A megfelelő biztonsági tanácsi képviselet

Van pár olyan szakterület, amelynek javasolt tagot delegálni a tanácsba annak hatékonysága érdekében. A javasolt területek, amelyektől természetesen adott iparági gyakorlat alapján el lehet, vagy el is kell térni a helyi viszonyoknak megfelelően: Az emberi erőforrás osztály, mivel naprakészek a foglalkoztatási adatokkal, fegyelmi ügyekkel, a magatartási kódexet is vélhetőleg ott kezelik. A jogi osztály tisztában van a szervezetre vonatkozó szabályozásokkal és törvényekkel. Az informatikai részleg műszaki adatokkal, fejlesztési, technikai javaslattal tudja támogatni a tanács munkáját. Természetesen a biztonsági osztálynak is képviseltetnie kell magát, aki a biztonsági szaktudást szállítja és jellemzően elnöki feladatot tölt be a tanácsban. A tanácsban az adott, delegált szervezeti egység vezetője ajánlott, hogy részt vegyen a felelős döntések meghozatalát annak gyorsaságát ez nagyban támogatja.

5. kritikus sikertényező: A tanács csoportdinamikai jellemzői

Bármelyik újonnan létrejövő csoportban működnek bizonyos folyamatok. Mindenki megpróbálja elfoglalni a saját pozícióját. Egyénre jellemző szerepeket is felvesznek a résztvevők. Van, aki hallgat, van, aki hallatni szereti a hangját, van, aki folyton csak kritizál,

stb. Fontos, hogy a most részletesen nem ismertetett csoportdinamikai állapotokon a tanács tagjai túljussanak és hatékony kommunikáció és csapatmunka valósuljon meg, valódi élő kommunikáció jöjjön létre. Minden jelenlévő tudja kifejteni és ki is fejtse az álláspontját.

6. kritikus sikertényező: Integráció a bizottságok munkájába

A valódi biztonságtudatos rutin kialakítása érdekében minden munkacsoportban, minden bizottságban meg kell, hogy jelenjen az információbiztonság képviselője. Hiszen minden folyamatba már a kezdetektől, tervezéstől számítva meg kell, hogy jelenjen ennek a szempontnak a képviselője. A hosszú távú és kitartó munka eredménye lehet az, hogy a felső vezetés is megfelelő komolysággal kezeli a kérdést és a szükséges forrásokat biztosítja. Ehhez szükséges riportok, beszámolók, értékelések formájában folyamatosan fent kell tartani a kommunikációt.

7. kritikus sikertényező: Korai létrehozás, növekvő siker

Jellemzően a 15-18 hónaposnál hosszabb kezdeményezéseket már hosszú távú projekteknek nevezik napjainkban. Ahhoz, hogy rövid és hosszú távon is sikeres lehessen a biztonsági program világos, teljesíthető apró részlépésekre (részcélokra) bontott célt érdemes kitűzni. Valami olyan apró, de mégis konkrét cél, ami viszonylag könnyen teljesíthető. Semmi sem támogatja jobban a program hosszú távú megvalósítását, a finanszírozási, támogatási lehetőségek megszerzését, mint a kezdeti sikerek. A kezdeti cél legyen olyan, ami

- támogatja az szervezeti célokat,
- legyen nagyon költséghatékony az indulásnál,
- időben legyen teljesítve,
- az egyeztetett költségvetésen belül legyen teljesítve,
- szállítsa (minimum azt) amit ígért.

8. kritikus sikertényező: Úton a tökéletesség felé

Vegyünk egy táncost, aki 15 éve minden nap gyakorol, tökélyre fejlesztette a tánctudását! És eljön a premier napja, amikor ezt bemutathatja. Mi történik, ha elvét egy lépést, vajon észreveszi a közönség? Valószínűleg nem, kivétel abban az esetben, ha megáll és újra és újra megpróbálja megtenni a nem sikerült lépést, ezzel felhívja a figyelmet a hibára. Ahogy egy fentebbi idézetben is szerepelt, a biztonság egy ideális állapot, amelyért

folyamatosan dolgozni kell. Voltaképpen lehet, hogy nem is létezik ez az állapot, csupán intézkedéseket tudunk tenni annak érdekében, hogy a kockázat csökkenjen, annak valószínűsége, hogy valamely, nem kívánt esemény bekövetkezik. Ettől még gyakorolni kell, tökéletesíteni a folyamatokat a nagy megmérettetésre készülve, azonban tisztában kell lenni azzal, hogy nem egy elérhető állapot, amiért dolgozunk. Az elérendő biztonsági szintet, hogy milyen alacsonyra kell leszorítani az esemény bekövetkeztének valószínűségét, a szervezet kockázati étvágya és a biztosított erőforrások határozzák meg. A tökéletesség ebben az értelmezésben a költségek és biztonsági implementációk egyensúlyban tartása a szervezeti, kockázatcsökkentési célok figyelembevételével.

9. kritikus sikertényező: A tanács fenntartó ereje

A tanács is emberek egy csoportja, így a résztvevő személyek is különböző állapotba kerülhetnek, például: leterheltség másik projektben, frusztráció, unalom, türelmetlenség és tehetetlenség is előfordulhat. Ha tisztában vagyunk azzal, hogy valami előfordulhat vagy bekövetkezhet, akkor sokkal könnyebb felkészülni a kezelésére és kezelni azt. Abban az esetben, ha a tanács nem kellőképpen hatékony, hogy folytassa a küldetését, akkor nem szabad hagyni, hogy értékes erőforrást, például az időt pazarolja azáltal, hogy nem termel kézzelfogható előnyöket. Előfordulhat, hogy új ötletekre, nézetekre, készségekre van szükség a csapatban. Ha ez megtörténik, akkor fontos újra áttekinteni a víziót, programot is, immár az új taggal, tagokkal felálló tanácsban.

10. kritikus sikertényező: A végfelhasználói tudatosság

A biztonságtudatossági képzés be kell, hogy ágyazódjon a szervezeti eljárásrendbe. A biztonsági szabályok megalkotásával az az üzenet, hogy ez üzleti döntés következménye és nem „csak” az informatikai osztályé, így nagyobb annak elfogadottsága is. Olyan szabályozási környezet felállítására van szükség, ahol minden egyes végfelhasználó megérti az általa betöltött szerepet. A tanács szerepe és lehetséges céljai, hogy

- segítsen ezen szabályzatok megértésében a felhasználóknak,
- üzenetet közvetítsen a vezetéstől az informatikai biztonság irányát megmutatva,
- ösztönzi a vezetést is a biztonság fenntartására.

Minden felhasználónak ugyanolyan gondossággal kell őrködnie a szervezet információs vagyona felett, mint ahogyan a zsebében lévő pénztárcájára vigyáz. Ezen állapot eléréséhez feltétlenül szükséges olyan program, amely segít megérteni a dolgozóknak a szervezeti struktúrát, annak működését és a hatékony egyensúlyt, a szervezet működése és a biztonsági célok elérése között.

3.3.2.1. Következtetések

A biztonsági tanács nagyban képes növelni az információbiztonsági stratégia elfogadását és a program végrehajtásának sikerét. Ezen kívül egy jó lehetőséget teremt több lehetséges csatornán keresztül a hatékony kommunikáció kipróbálására és folytatására a szervezetben. A fentebb megfogalmazottak alapján érdemes a kezdeti sikereket kommunikálni, ezen kommunikációval kiterjeszteni a stratégiát nagyobb léptékű projektekre is. El kell érni a bizottságokban és az egyéneknél a személyes bevonódást és érdekeltségek. Azaz ne csak jelen legyenek a megbeszéléseken, hanem aktívan működjenek közre. Bizonyos szervezeti csoportoknak mindenképp reprezentálniuk kell magukat ebben a tanácsban, de lehet eseti csoporttagokat is meghívni az állandó tagokon kívül. Ugyanakkor azzal is tisztában kell lenni, hogy nem a tanács a megoldás vagy garancia a program sikerességére. Bármely szervezet életében lehetnek olyan időszakok, amelyek jelentősen befolyásolják a tanács munkáját. Például átszervezések, költségvetési átcsoportosítások, nagyprojektek. Ezek azonban bármely szervezetben a normál működés részeként felléphetnek. Itt kiemelt az információbiztonsági vezető felelőssége, mivel ezen helyzetekben is ugyanaz a feladata akár a vezetés időleges támogatásának hiányában is, akár annak támogatását és a tanács együttműködését élvezve.

Végezetül a biztonsági vezetőnek értékelnie kell tudni saját magát is, saját elkötelezettségét a programban, a szervezeti kultúra hatását a biztonsági programra. Meg kell tudnia határozni hol tart most a szervezet. Elsőre talán, a munka kezdetén nem tűnik kényelmes megoldásnak a biztonsági tanács létrehozásával kapcsolatosan befektetett energia és munka. Azonban el kell kezdeni a tanács és a tagok összeállítást a jog, informatika, technológia, a HR, további szervezeti egységek területén még ma!

Jelen fejezetben a változáskezelés és életciklus kezelésen keresztül vizsgáltuk a folyamatokat. A változáskezeléssel részletesen foglalkoztunk a kockázat feljegyzési követelményeknél, így most csak utalás szintjén pár pont kerül kiemelésre. A magyar

fordításban elégedettségi riport követelményként megjelenő fogalmat a nemzetközi irodalom compliance, azaz megfelelőségként használja gyakrabban. A megfelelőség kapcsán a jogszabályi és egyéb szabályozási környezetnek, a munkaszervezeti céloknak való megfelelés kerül előtérbe. Ennek kezelésére vonatkozólag az életciklusokba ágyazás képes hatékony megoldást adni. A szigorúan vett elégedettségi riport sok szempontból hasonlóságot mutat a változáskezelési dokumentum menedzsmenttel. Azaz megfelelő szabályozási eljárások mentén adatokat szolgáltatunk a teljes életciklus alatt a RACI szerinti feleknek. A riport követelményekkel kapcsolatos gondok, figyelembe véve a kockázatkezelési problémákat, gyakran oda vezethetőek vissza, hogy

- nem épülnek be a folyamatok életciklusába a kockázatkezelési eljárások, riportok, ellenőrző pontok
- nem megfelelő a RACI táblázat, vagy az adott eljárás, amely szabályozza a címzettet és annak feladatait
- a változáskezelési eljárás valamiért nem működik,
- olyan területen történik változás, amely nincs megfelelőképpen lefedve folyamatokkal (gap)[26]

Ezért a kockázatkezelésnek és változáskezelésnek be kell épülnie az életciklusokba. Ha változás történik bármely folyamatban, akkor azt változáskezelőn keresztül be kell jelenteni és el kell végezni a folyamatban és érintett folyamatok figyelembevételével a kockázatkezelést. Ezen kívül a folyamatra érvényes szabályozás szerint bizonyos időnként (legalább évente) egyébként is el kell végezni újra a folyamatok áttekintését és a kockázatértékelést. Ezen folyamatnak fontos szerepe van abban, hogy az esetleges negatív hatások minimalizálhatóak legyenek.[27] Az SDLC[28] által definiált öt állapotot[29] az alábbi ábra mutatja. A kockázatkezelés annak érdekében, hogy a megfelelőségi, elégedettségi riport követelmények működőképesek legyenek és fenntartsák a szervezet folyamatainak biztonságos működését, iteratívan, ismétlődően, az életciklusba épülve kell, hogy megvalósuljanak.

[26] Nincs lefedve folyamatokkal, vagy a folyamat nem jól megtervezett, végső soron a változás nincs kezelve.
[27] NIST 800-30-as kiadványa további részletes információkat tartalmaz.
[28] System Development Life Cycle öt állapotot definiál.
[29] 1) Kezdeményezés, 2) Fejlesztés vagy beszerzés, 3) Végrehajtás, 4) Üzemeltetés vagy karbantartás, 5) Megsemmisítés

SDLC fázis	Fázisjellemzők	Támogatja a kockázatmenedzsment tevékenységét
1. fázis - kezdeményezés	Kifejeződik az IT rendszer iránti igény, amelynek célját és tartományát dokumentálják	Az azonosított kockázat segít a rendszerkövetelmények megállapításában (stratégiai és biztonsági)
2. fázis - fejlesztés vagy beszerzés	Az IT rendszert megtervezik, megveszik, programozzák, létrehozzák, vagy egyéb módokon elkészítik	Az ebben a fázisban azonosított kockázati tényezők segítik az IT rendszer biztonsági analízisét, mely felépítési és tervezési cserékhez vezethet
3. fázis - végrehajtás	A rendszer biztonsági tulajdonságait beállítják, üzembe helyezik, tesztelik és hitelesítik	A kockázatmenedzsment folyamat támogatja a végrehajtást, annak igényeit a működési környezetének modelljében. A működésbe lépés előtt meg kell hozni a kockázatokra vonatkozó döntéseket
4. fázis - üzemeltetés vagy karbantartás	A rendszer ellátja funkcióit. Alapesetben rendszeres javításon és változtatásokon esik át (hardverből szoftver és vice versa), illetve egyéb, nem ilyen feltűnő módon változtatják meg	A kockázatmenedzsment folyamatai a rendszer periodikus újraengedélyezései alatt zajlanak (vagy olyankor, amikor a már működő rendszerben jelentős változtatásokat hajtanak végre, például: új kezelőfelület)

5. fázis - megsemmisítés	Ebben a fázisban történik az információ, a szoftver és a hardver beosztása. A tevékenységi körök közé tarozik a mozgatás, archiválás, elpusztítás, megsemmisítés.	A kockázatmenedzsment folyamatai olyan részegységeket érintenek, melyeket kidobnak vagy kicserélnek, így biztosítva, hogy a hardver és szoftver elemek, melyektől megszabadultak, szisztematikusan és biztonságosan legyenek kiváltva és cserélve

3. ábra: SDLC fázisok jellemzői, ISACA, CISM Review Manual 2013, Chapter 2, page 123, Information Risk Management and Compliance

4. Hatékony projekttervezés és menedzsment[30]

Mottó:
„Egyetlen ismeret van, a többi csak toldás:
Alattad a föld, fölötted az ég, benned a létra.”[31]

4.1. Bevezetés

E könyv olvasói is saját bőrükön érezhetik nap, mint nap, hogy az informatika rohamos fejlődése révén újabb és újabb alkalmazási, támogatási lehetőségek jönnek létre, amelyek a munkaszervezeti célokat, felhasználókat, munkájukat képesek támogatni. Ilyen szempontból vizsgálva nem nagyon lehet különbséget találni kormányzati, vállalkozói vagy egyéb iparági szegmensek között, legfeljebb a konkrét motiváló tényezőkben lehet különbség. Az is kijelenthető hogy az informatikai projektek nem csak számosságuk, de az adott szervezet céljaink és jövőbeli sikerességének tekintetében is komoly, meghatározó tényezővé váltak. A „miért van szükség projektekre” kérdésre a válasz egyértelműnek tűnhet, hiszen a szervezet stratégiai céljainak eléréséhez projektek sokaságát valósítja meg a változó körülményekhez való alkalmazkodás érdekében. Ezen folyamatokban pedig egyre nagyobb teret nyer az informatika, mint a munkafolyamatokat segítő eszköz.
A vezetés szintjei munkaszervezetenként változó módon különülnek el. Logikailag azonban egészen biztos megkülönböztethetjük a vezetés egyik dimenziójaként az operatív menedzsmentet, amely az aktuális és közvetlen feladatok eredményes teljesítését hivatott biztosítani. Azonban tudhatjuk, hogy nem csak ilyen feladatok léteznek, hanem időben újabb és újabb (tervezett) célállapotok jelennek meg minden szervezet életében, jövőképében. Ezt a dimenzióját a vezetésnek sokkal inkább stratégiai menedzsmentnek nevezhetjük. A szervezet jövőbeni működőképessége nagymértékben a stratégiai célok realizálásának a mikéntjén múlik. A stratégiai célok megvalósítása ugyanis egy bizonyos időszakra a napi, operatív tevékenységek részévé válik és jelentősen befolyásolja a szervezet működésének eredményességét. Ezek megvalósítása tehát nem különíthető el, gyakran párhuzamosan, egymással valamilyen átfedésben valósulnak meg. A stratégia realizálásának azonban van jól

[30] Felhasznált irodalom: Görög Mihály, Ternyik László: Informatikai projektek vezetése, Kossuth, 2001. ISBN 963-09-4227-5
[31] Weöres Sándor

körülhatárolható, komplex és egyszeri részfeladata is. Ezek különböznek mind a stratégiai, mind pedig az operatív menedzsmenttől. Ez a projektmenedzsment. A projektmenedzsment a stratégia célok realizálását valósítja meg annak napi szintű, operatív működési területre történő transzformálásával. A projekt a fentiek alapján olyan tevékenység, amely a szervezet számára egyszeri, komplex feladatot jelent, meghatározottak az időbeli és egyéb erőforrásbeli korlátai (pl.: költségek). Továbbá definiált a célja vagy eredménye, annak elérésére irányul és az adott időben még nem létezik a szervezet számára. A projektmenedzser pedig az a személy, akinek ez hatásköre és egyben felelőse is a projektnek, a sikeres teljesítésnek. A vezetés három dimenziója tehát az operatív, a stratégiai menedzsment és a projektmenedzsment. A konkrét projekt pedig definiálható a célként elérendő eredménnyel, a teljesítés időtartamával, és erőforrásaival (költségkeretével). A projekteket számos szempont szerint lehet csoportosítani komplexitás, a vezetés helye és cél vagy részcélok tekintetében is.
Feltehetjük a kérdést, hogy mit értünk informatikai projekten. Napjainkra ritka a tisztán informatikai projekt, jellemzően valamely részfeladat informatikai eszközzel történő támogatása, az információáramlás, a tudásfeldolgozás, a rögzítés számítástechnikai eszközökkel történő támogatását jelenti. Azaz jellemzően technológiai elemek keverednek szervezési, folyamatszervezési, humán változáskezelési elemekkel. Fontos szempont a projektek sikerességének szempontjából, hogy mennyire mérhető, azaz kvantifikálható-e és mennyire. Minél kevésbé tehető mérhetővé számszerű értékekkel a projekt, annál inkább fennáll a veszélye, hogy a kitűzött projektcéltól eltérő eredmény jön létre. Ennek lehetséges az elkerülése, ha a projektdefiníciós tervben megfelelő kontrollok kerülnek alkalmazásra. A projektdefiníciós terv a projekt életciklusában többek között meghatározza és rögzíti a végrehajtandó feladatot (projekteredmény, költség és erőforrás korlátok, határidő). Ezáltal alapjául szolgál a projektmegvalósítás stratégiai kidolgozásához, a teljesítésre vonatkozó projektterv elkészítéséhez, a projektkontrollhoz (változáskezelés, teljesítés elfogadás kritériumai), végül a projekt befejezésekor elvégzendő értékeléshez, a sikerességi kritériumok mértékének megállapításához.

4.2. A projekt teljesítése

A projekt teljesítése akkor mondható teljesen eredményesnek, ha megvalósulnak az elsődleges projektcélok és eközben hozzájárul a szervezet érvényes stratégiai céljainak eléréséhez. A teljesítés során azonban számos körülmény adódhat, amely valamilyen módon

és eltérő mértékben eltérítheti az eredetileg kijelölt elsődleges célok tekintetében a projektet. Egyfajta felosztás szerint ezek két nagy csoportra oszthatók: változtatások és módosítások valamint eltérések.

A változtatások tekintetében jellemzően szándékolt eltérítést értünk, amely a projekt elsődleges céljait érinti. Nem teszünk, azonban különbséget illetve nem vizsgáljuk, hogy ezt külső vagy belső okok eredményezik-e. Az eltérések valamilyen nem szándékolt különbséget jelentenek a tervezett és a tényleges állapot között. Ebből következik, hogy az eltéréseket igyekszünk elkerülni, hatásait minimalizálni. A projekt folyamán ciklikusan futtatott projektkontroll segíthet a célok és források egyensúlyban tartásában, a projekt mérföldköveinek időbeliségének ellenőrzésében. A legegyszerűbb projektkontroll lépések

- a normák rögzítése
- információk gyűjtése
- elemzés
- korrekciós intézkedések,

melyet körfolyamatként értelmezve ciklikusan ismételni szükséges. A projektkontroll során keletkező információkat az operatív értekezleteken gyorsan át lehet tekinteni, a szükséges intézkedések meghozatalára is lehetőség nyílhat. Ilyen lehet a pótlólagos információk gyűjtése, döntési alternatívák értékelése is. Az operatív értekezlet jellemzően heti gyakoriságú, főbb funkciói:

- gyors információcsere,
- problémafeltárás, illetve megoldási javaslatok kialakítása és értékelése,
- az operatív döntések előkészítése,
- előző operatív döntések követése, esetleges módosítása,
- utasítások közlése.

4.3. A projekt támogatása

A projekt logikai támogatása megvalósulhat valamilyen módszertan alkalmazásával, amely keretet teremt az eljárásoknak,valamint hatékonyan támogatható ilyen célra fejlesztett szoftveres megoldásokkal is. Bizonyos elterjedt alkalmazások is kínálnak erre megoldásokat,

valamint léteznek külön ilyen célra fejlesztett nyílt forráskódú és fizetős alkalmazások is. Hosszabb távú, nagy létszámú, sok mérföldkővel rendelkező projektek esetén ajánlott valamilyen szoftveres támogatás alkalmazása, valamint az előrehaladási jelentések, operatív értekezletek egyéb dokumentumok kezelése dokumentumkezelő rendszer. Ilyen rendszerben meghatározható adott dokumentum, annak változtatása esetén az, hogy milyen szabályok, utasítások hajtódjanak végre.[32]

4.4. Értékelés, avagy mikor sikeres egy projekt?

Talán azon kívül, hogy hogyan érhető el ez az állapot, a másik legfontosabb kérdés, hogyan dönthető el az állapot megléte, a teljesítmény vagy teljesítésértékelés, a teljesítés elfogadása. Az értékelés a projektciklus záró fázisa, melynek során három fő tevékenységcsoport kerül előtérbe:

- a projekteredmény értékelése, egybevetése a szervezet stratégiai céljaival
- a projekt megvalósítási folyamatának elemzése a projektmenedzsment sikeressége szempontjából
- a tanulságok összegyűjtése a projekt folyamán, a projekteredmény létrehozásához kötődő műszaki, szakmai tapasztalatok összegzése és újrahasznosítás céljára történő előkészítése (ennek kapcsán a szervezeti tudáskezelésről még bővebben lesz szó.)

Meg kell jegyezni, hogy egy projekt sikeressége, a siker vagy kudarc kialakulásához vezető tényezők nem mindig számszerűsíthetőek, sőt a sikerfaktorok kiválasztása is meglehetősen önkényes alapon történhet. Elegendő arra gondolnunk, hogy bár szervezeti célok vagy a menedzsment szempontjából sikeresen bevezetett rendszer nem biztos, hogy a folyamatban résztvevők, azzal dolgozók számára élhető környezetet biztosít, nem támogatja kellőképpen a munkafolyamatot. A projekt sikerességét legalább három különböző szinten vizsgálhatjuk. Az első szintje a már többször megfogalmazottak alapján a projekt céljai szerinti megítélés. Ebből a szempontból a projektmegvalósítás akkor sikeres, ha az előre definiált eredmény (teljesség, funkcionalitás, minőség, határidő, erőforrások, stb.) mentén megvalósult. Azonban túllépve ezen a leegyszerűsített vizsgálaton, ebből nem következik feltétlenül, hogy sikeres a

[32] Automatikus változáskezelés, érintettek automatikus értesítése, egyéb kényelmi és automatizálható funkciókkal rendelkezhet a program.

projekt abban az esetben, ha ezen értékeket produkálta. Azaz a tervezett időtartam alatt és az előre meghatározott költségkereten belül valósult meg. Itt két dolgot kell kiemelni, az egyik a szervezet stratégiai céljaihoz való illeszkedés (amely időközben akár változhatott is), valamint a funkcionalitás, hiszen több száz felhasználója lehet egy rendszernek, akik érdekeltségi körök alapján különböző halmazokba rendezhetők.[33]

A siker megítélésének második szintjét a stratégiai célokkal való egybevetés kell, hogy képezze. Tehát, bár a projektet meghatározott stratégiai célok hívták életre, de az esetlegesen hibás célkitűzések a projekt teljesítése során nem kerültek javításra, vagy a reális és megalapozott célkitűzések időközben érvényüket vesztették, akkor mindenképpen a projekt folyamán ezek módosítása szükséges. Bármelyik esetről van is szó, ha ezek a módosítások elmaradnak, akkor a szervezet szempontjából ez elfecsérelt erőforrás, a projekt azért nem tekinthető sikeresnek, mert nem szolgálja a szervezet valós stratégia céljait.

A harmadik szempontból vizsgálva, ha a projekt valós stratégiai célokat elégít ki, teljesítése megfelel az elvárásoknak, akkor időben visszamérve a megítélésben fontos tényező, hogy mennyire adoptálódik a rendszer a munkaszervezetben a munkafolyamatokba egyes érdekcsoportok, vagy rész-szervezetek esetében. A későbbiekben még visszatérünk arra, hogy a hatékony információbiztonsági program és annak vezetője hogyan tud valós adatokat szerezni a projekt sikerességéhez. Összességében tehát a projekt sikerességének mértékét három dimenzióban érdemes vizsgálni:

- a projektet meghatározó elsődleges projektcélok,
- az érvényes szervezeti stratégia,
- a projektben érintett érdekcsoportok.

A projektmenedzser elemi érdeke a projekt céljainak megfelelő menedzselése, hiszen annak sikertelensége esetén, bár hibásan, de gyakorta a projekt tulajdonosával, menedzserével azonosítják a sikertelenség okait. A projekttulajdonos feladatai roppant szerteágazóak lehetnek, néhány olyan általános javaslat létezik azonban, amely nagyban hozzájárulhat a sikerhez.

[33]Például egy vezetői információs rendszerben megjelenő naprakész adatokhoz a szervezet minden főbb egységénél napi szinten szükséges adatmezők kitöltése. Gondoljunk csak bele a legelemibb elvárásba munkavállalói szempontból: egy adatot legfeljebb egyszer kelljen (kézzel vagy más módon) rögzíteni. Minden olyan eljárási változás amely többletfeladatot indukál és kommunikációval nem támogatható vélhetőleg a szervezet ezen részében nem fog sikeresnek számítani. Ezáltal könnyen olyan eredményeket képes generálni, melynek eredményeképpen az információs rendszerben megjelenő adatok nem lesznek naprakészek, és ez hatással lesz az egész projektre.

Kommunikáció az érintettekkel. Érintett nem csak az adott osztály vezetője lehet, hanem olyan, aki értékes információkkal, visszajelzéssel szolgálhat, akár feladat tényleges végrehajtója (pl.: a példánál maradva az adatrögzítésre kötelezett munkavállaló is). Javasolt megfelelő időt szánni az értékes, kvalitatív visszajelzésekre is a projekt folyamán. Ezen kívül fontos a projekt aktuális állása, célkitűzései, kitérve és megmutatva, hogy az adott alprojektek, munkafázisok hol szolgálják majd a közös érdekeket. Az információbiztonsági programnál ennek egy lehetséges módja azt megmutatni, hogy a tudatosság nem csak a munkahelyen, hanem a magánéletben is rendkívül fontos. Hiszen ugyanolyan visszaéléseknek van kitéve a munkahely falain kívül is a munkavállaló, ahol már esetleg nem védi levelezőrendszerét, számítógépét a vállalati rendszer. A projekttel kapcsolatos, operatív szint feletti teendők:

- Projektbehatárolás, mind terjedelmileg, mind pedig az időtartam és költségek tekintetében. Minden tekintetben törekedni kell a mérhetőségre.
- Olyan stratégia kialakítása, amely támogatja a projektet abban, hogy a felelősségek és kockázatok összhangban legyenek a szervezet és a projekt struktúrájával.
- A megvalósítás folyamán keletkező adatok, információk és eredmények folyamatos feldolgozása és összevetése az érvényes szervezeti stratégia célkitűzéseivel. A projekt bizonyos pontjain különösen nagy jelentősége van ennek, előrehaladási jelentés, döntési vagy elágazási pontoknál.
- A folyamatban lévő projektek módosítása, változtatása, akár törlése, amennyiben azt a körülmények indokolttá teszik.
- A megvalósult (rész) projekteredmények integrálása a szervezet operatív (napi) működési folyamataiba, ezek további nyomon követése.

Projektmarketing eszközökkel a projekt és projekteredmény elfogadtatása az érintettekkel (külső és belső érdekcsoportok). Ki kell emelni, hogy nagyjából a projekt életre hívását követően meg kell tenni ez ügyben az első lépéseket, a stakeholderek[34] bevonása nem csak értékes információforrás a projekttervezésben, de további kommunikáció alapkőletételét is jelenti. Amennyiben erre nem kerül sor a projekt indításakor, úgy ettől az időponttól távolodva egyre nehezebb az ilyen támogatás megszerzése a folyamatban lévő projekt

[34] érintettek

számára. Az információbiztonsági program szempontjából ki kell hangsúlyozni, hogy az nem kezelhető szigorúan egy projektként, hanem projektekre lehet legfeljebb bontani. Ennek az az oka, hogy életciklusokra, ellenőrzési pontokra tagolódik és az egész keretrendszer filozófiája a változáskezelésen és az iteratív folyamatokon nyugszik. Természetesen egy – egy változáskezelést, kockázatértékelést, valamilyen részfolyamatot kezelhetünk és kell is kezelni a szükséges projektmenedzsment eszközök segítségével, felhasználásával. Az információbiztonsági program hatékonysága a kockázatok csökkentésével, a szervezeti célok elérésének támogatásával, az egyenszilárdság, a tudatossági szint alapján jellemezhető, mérhető.[3536]

4.5. Szervezeti tudásmenedzsment

A minden szempontból sikeresen megvalósult projekt során vélhetőleg számos értékes tapasztalat halmozódott fel, mind a projektmenedzsernél, mind pedig az érdekelteknél, résztvevőknél. A szervezet érdeke, hogy a rögzíthető ismereteket, a fejekben lévő tudást leírható tudássá kell alakítani. Különösen jelentős ez napjainkban, amikor a szervezetek információgazdálkodása központi kérdés, a szervezeti (adat)vagyon nagy részét az információ teszi ki. Sok esetben valamilyen fenntartási idővel vállalt projekteknél fontos a kapcsolatok megőrzése. Munkaerő fluktuáció esetén is rendelkezésre kell, hogy álljon az adott információ.[37] Ennek elmaradásával, vagy puszta késlekedés esetén is, annak anyagi vonzatával is számolni kell.
A rögzítendő információknak, tapasztalatoknak három fő csoportja van:

- a projektmenedzsment szakmai tapasztalatai,
- a projekt tárgyával kapcsolatos szakmai tapasztalatok,
- egyéb.

[35] A mérésre a SANS nemzetközi szervezetnek léteznek módszerei, http://www.sans.org/
[36] Lehetséges irodalom: Illéssy Miklós – Nemeslaki András – Som Zoltán, Elektronikus információbiztonság-tudatosság a magyar közigazgatásban, Információs Társadalom, ISSN 1587-8694
[37]Például: módosítási vagy fejlesztési igény, hibabejelentés esetén, konkrét példával élve a törvényi változások miatt valamilyen szoftverben kötelező képletmódosítást kell eszközölni, ez azonnal beavatkozást igényelhet.

4.6. Egyéb információk

Az első csoportba tartozó tudás az, amit a projekt során a projektmenedzsmentről tanultunk. Tehát a projekt vezetője vagy vezetői szakmailag mi újat tanultak a szakmájukról a projekt megvalósítása során. Kevés olyan beszámoló létezhet, amikor ez a beszámoló űrlap üresen maradhat. Ennek tartalmilag a mérhető mutatóktól a nem mérhető a szervezetre jellemző egyes érdekcsoportokkal folytatott egyeztetésekkel kapcsolatos tapasztalatokig kell terjednie a kockázatok elemzéséig. Ez nemcsak a munkaerő fluktuációja miatt, hanem a későbbi hasonló projektek kapcsán és az esetleges projektellenőrzés szempontjából fontos. Könnyű belátni, hogy reálisan nem készíthető el ilyen dokumentum hónapok vagy évek távlatából. Ezt valamilyen gyakorisággal a projekt folyamán is vezetni érdemes, annak végén lezárni és összegezni.

A második csoportba sorolható a projekt tárgyával kapcsolatos szakmai tapasztalatok rögzítése. Ezek lehetnek technológiai adatok, felhasználható részeredmények, szoftvermodulok. Információbiztonsági program esetén pedig olyan megfigyelések, amelyek a munkaszervezetre, csoportokra jellemzőek. Működő és nem működő példák egyaránt hasznosak lehetnek a későbbiekben. Hiszen az ilyen információk, tapasztalatok reprodukálása erősen költség és humánerőforrás igényes.

Az egyéb kategória definícióját tekinthetjük egy egyéni, személyes beszámolónak. Úgy könnyű talán megragadni, hogy a projekt zárásakor, a résztvevők formális felszabadításának megtörténtét követően nagy jelentősége van a humán faktornak. Azaz a projektcsapat szociális igényeit is kielégítve a projekt formális zárásaként olyan projektzáró – rendhagyó operatív – értekezlet megrendezésére kerülhet sor, amikor a személyes beszámolókból, fényképekből készült összeállítás mellett a projektzáró dokumentum főbb megállapításait is ismertetni lehet. Itt nyílik lehetőség a tapasztalatok szélesebb körben történő, informális átadására is.

Meg kell jegyezni, hogy a stratégiai célok akciótervekké, majd azok projektekké alakítása szolgálja mind a megvalósíthatóság, mind a szervezeti célokat is. Gyakran érdemes részprojektekre bontani egy-egy projektet annak érdekében, hogy minél nagyobb valószínűséggel legyen sikeresen és a rendelkezésre álló kereteken belül teljesíthető. Ismét az információbiztonsági terv kommunikációját hozva példának, vizsgáljuk meg ennek összetettségét! A gyakorlatban a szabályozás valamilyen vaskos dokumentum, amely elég ritkán tekinthető olvasmányosnak. A célközönség a munkavállalók és beszállítók, partnerek is. Olyan csoportok, akik egymástól élesen elkülöníthetőek, mert például más területen

érdekeltek, más munkafolyamatokban vesznek részt. Tehát, bár egyszerűnek tűnhet az információbiztonsági program propagandájának segítése informatikai eszközökkel (e-mail, videó, képernyővédő, stb.) azonban azon (akár kiszervezett) munkavállalók esetében, akik (napi szinten, vagy egyáltalán) nem használnak informatikai eszközöket, ez a csatorna nem jelent kapcsolódási pontot. Tehát az egyes érintettek körét megvizsgálva, olyan csatornákat kell találni, amely minden munkavállalóhoz képes eljuttatni azon a nyelven az üzenetet, amely korrelál az adott érdekcsoportéval. Ennek érdekében egyes halmazokhoz kell meghatározni a megfelelő kommunikációs csatornákat. A projekt támogatására napjainkban már számtalan megoldás létezik. Ilyen szempontból a menedzsment munkájának támogatására speciális szoftverkomponensek is rendelkezésre állnak, amellyel idő és mérföldkövek szempontjából vizuálisan lehet áttekinteni nagyobb projekteket. Ilyenek Gantt, LOB (Line of Balance) CPM, PERT diagramok. Ezt jól kiegészítheti a feladat, felelősségi mátrix elkészítése, amely valamilyen időintervallumot alapul véve (pl.: heti frissítést) az előrehaladási állapotot is jól tudja reprezentálni.

4.7. Kockázatkezelés a projektmenedzsmentben

A projektmenedzsmentben a kockázatkezelés kettős célt szolgál. Egyrészt a hatékonyabb megvalósítást teszi lehetővé, hogy a reálisabban, kevesebb kockázattal (idő és költségkeret) elérhető, reálisabban megvalósítható projekteredmény kitűzését teszi lehetővé, ezzel optimalizálja a projektstratégiát. Másrészt gazdasági szempontból jelentősen hozzájárul a reális gazdasági-pénzügyi értékeléshez, a választott pénzügyi döntésnél a kockázatokra való rámutatással.
A kockázatkezelési politika nem csak a döntéshozók kockázatokkal kapcsolatos reakciója, hanem azon cselekvési módok összessége, amelyeket a kockázatok váltanak ki a döntéshozókból. A kockázatkezelési politikai eszköztára a projektmenedzsmentben:

- a kockázatok elkerülése,
- a kockázatok csökkentése,
- a kockázatok áthárítása
- a kockázatok megosztása.

A gyakorlati tapasztalatok alapján jellemzően a kockázatkezelési megoldások valamilyen kombinációja kerül alkalmazásra. A kockázatok elkerülése voltaképpen azt is jelentheti, hogy a túlságosan nagy rizikóval járó tevékenységet a továbbiakban nem alkalmazza a szervezet, vagy a projekt során nem kerül felhasználásra. Ez a gyakorlatban kevéssé alkalmazható, hiszen vélhetőleg szükséges az adott tevékenység a szervezet egésze szempontjából, de érdemes minden tényezőt megvizsgálni. Általánosságban a kockázat elkerülése elérhető:

- elsődleges döntések meghozatalának segítségével,
- a projektstratégia megfelelő koordinációjával.

A kockázatok csökkentése sok tekintetben hasonló az elkerüléséhez, azonban itt sokkal nagyobb szerep jut a projektstratégiának. További lehetőség a még pontosabb kvantitatív és kvalitatív adatok beszerzése a mérlegelés pontosságához. Ilyen kockázatcsökkentő módszer lehet a kalkulációs tartalékkeret képzése, szerződéskör a vis major esetekre történő kitérés. Valamint elképzelhető független minősítő alkalmazása is, ez akár a teljes projektmenedzsment kiszervezését is jelentheti. A kiszervezett projektvezetés egyes vélemények szerint olyan hátránnyal indul, hogy nem ismeri annyira a cég belső folyamatait, struktúráját, ennél fogva a célok rendszerét se. Ebben az esetben különösen nagy jelentősége van a folyamatos dokumentálásnak. Általánosan a kockázatok csökkentése, mint kockázatpolitikai magatartás megvalósulhat:

- a projektstratégia révén,
- idő – és költségtartalékok képzésével,
- helyszínre, körülményekre, valamilyen egyéb jelentős tényezőre vonatkozó részletesebb információk beszerzésével,
- alternatív megoldásokkal.

A kockázatok áthárítása talán a leggyakrabban alkalmazott eszköz. Ennek során a kockázat átkerül

- a projekttulajdonostól a külső közreműködőhöz (kötbérezés valamilyen tényezőre),
- a közreműködőktől az alvállalkozóhoz (kötbérezés továbbhárítása),
- minden közreműködőtől a kezeshez (bankgarancia),

- minden közreműködőtől a kezeshez.

A gyakorlatban a közreműködők kockázatvállalási képességeinek korlátai miatt lehet, hogy nem ez az optimális megoldás, ezért szintén gyakori megoldásként a kockázatok megosztására kerül sor. Ilyen esetre példa lehet a projekt időtartama alatt, mondjuk inflációból eredő kockázatokra átalánydíjas elszámolás, vagy a szerződésbe foglalt olyan passzus, amely a projekttulajdonos és a vállalkozó között osztja meg a kockázatokat.
Korábban említésre került, hogy ezek a megoldási lehetőségek nem mindig vegytisztán jelennek meg a projektekben. Gyakran egy-egy projektciklushoz, annak megfelelő fázisához kapcsolódnak, mivel eltérő kockázatok kerültek azonosításra, így más kockázatkezelési megoldást szükséges alkalmazni. Tehát az eddigi modellekhez hasonlóan, részfolyamatokra is iteratív módon alkalmazhatóak az ismertetett stratégiák.

4.8. Az információbiztonsági program eredményei

A hatékony információbiztonsági programnak el kell érnie a kitűzött és meghatározott célokat, melyek a stratégiában kerültek meghatározásra. Ehhez elengedhetetlen, hogy ezek valóban jól specifikáltak és mérhetőek legyenek, bár tisztázásra került már, hogy léteznek nem számszerűsíthető tényezők is. A szakirodalom hat területre próbálja meg összefoglalni a programmal kapcsolatos logikai szerkezetet. Mindenekelőtt azonban kiemeli, hogy az információbiztonsági programnak a fejlesztés során hozzá kell simulnia, igazodnia és szoros logikai kapcsolatba kell kerülnie a technológiával és a folyamatokkal. Tehát a programot meg kell vizsgálni fizikai, funkcionális, üzemeltetési komponensek szempontjából is, annak érdekében, hogy minél jobban elérhetőek legyenek a definiált célok.

1. Stratégiához igazítás

A biztonsági program összehangoltan képes támogatni a szervezeti célokat.A biztonsági program folyamatokba történő implementálása, figyelembe véve a szervezeti célokat pedig folyamatos bemeneti feltételeket biztosíthat a biztonsági program irányításához. Tehát nagyon fontos, hogy a biztonsággal kapcsolatos megfelelő visszajelzések eljussanak a folyamatgazdákhoz és érdekeltekhez. Ezek lehetnek a projektek előrehaladásával kapcsolatos információktól a kockázatokig terjedő információk, amelyek befolyással lehetnek az egész szervezetre. A program végrehajtásakor a világos, egyértelmű kommunikáció és a

változáskezelés irányítási tapasztalatok, stratégiák és gyakorlatok az üzleti követelményeket elégítik ki. Egyértelműen meg kell határozni és világosan kommunikálni az elfogadott biztonsági szintet, azt hogy ez milyen kockázat – per – költség kompromisszum által jött létre.

2. A kockázatmenedzsment

A biztonsági program fő célja a kockázatot az elfogadott szintre csökkenteni. Ezek meghatározásra kerültek a stratégiában, kockázatértékelési módszerekkel. Azonban a kockázatok és fenyegetettségek állandóan változnak a program fejlesztése és végrehajtása során és ennek számos oka lehet (ez a változásokból is következik.) Ezért is fontos, hogy folyamatos legyen a kockázatok értékelése és kezelése a program kivitelezése során is.

3. Értékteremtés

Az információbiztonsági programnak a szervezeti céloknak megfelelő, azzal összhangban lévő eredményeket fel kell tudnia mutatni, ez egyértelműen elvárás. A megfelelő szintű szabályozás és kockázatkezelés hatékonyan és eredményesen kell, hogy megvalósuljon. Ehhez jó tervezés szükséges, projektmenedzsment ismeretek az első sikerek elérése érdekében, amelyek mint arról már szó volt, stabil alapot teremthetnek a további munkához.

4. Erőforrások kezelése

A program fejlesztése, kivitelezése során számtalan erőforrást használunk fel. Ide tartozik a saját munkaidőnk, de általában véve az emberek, technológiák, folyamatok is. Ezekkel optimálisan gazdálkodni kell tudni. Annak érdekében, hogy a rendelkezésre álló erőforrásokat jól fel tudjuk használni, jól meg kell tervezni a programot. (időzítés, a személyzet megfelelő előképzettsége és készségek megléte).[38]

5. A területek biztosítása

A biztonsági programban lehetőség van olyan fokozott biztonsági pontok beépítésére, amelyek kapcsolatot teremtenek más, kiegészítő szolgáltatókkal. Ez gyakran meg is valósul, akár ezeken a területeken is: informatikai biztonság, audit, könyvvizsgálat, emberi erőforrás (például: kiválasztás, fejvadászat), fizikai biztonság, adatvédelem, jogi terület,

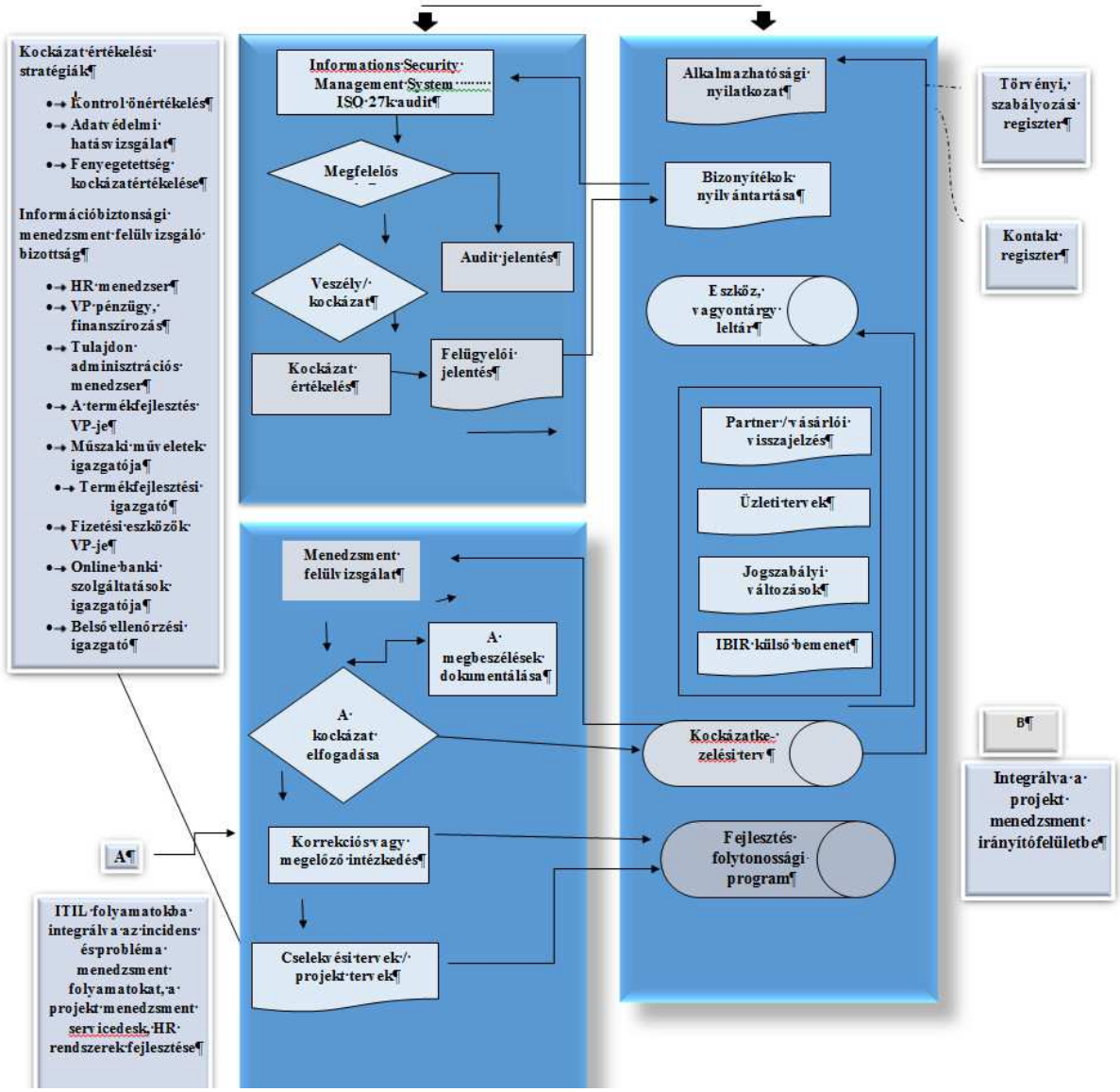
[38] Gyakori buktató, hogy megfelelő informatikai alapok és előképzettség nélkül olyan anyag kerül oktatásra, amely ezen tudás meglétét feltételezi.

minőségbiztosítás, vagy más egyéb területeken is, amelyek közvetetten vagy közvetlenül hatással lehetnek a biztonságra, a szervezet védelmére.

6. A teljesítmény mérése

A teljesítmény mérhetősége érdekében az információbiztonsági stratégia fejlesztése során fontos változók monitoringjának és mérési követelményeinek rendszere meghatározásra kellett, hogy kerüljön. A mérési, értékelési folyamat abban is segítséget adhat, hogy hiányosságokra, hibákra derüljön fény a biztonsági tevékenység során, valamint visszajelzéssel szolgálhat a folyamat során megoldott kérdésekkel kapcsolatban, segíthet a terv sikerességének kommunikációjában is.

A hatékonyság kimutathatósága érdekében tehát a tervezés során kell definiálni olyan tényezőket, mérési pontokat, amelyek visszajelzéssel szolgálhatnak a folyamatban. Ezek alapján nem csak mérhetővé válik a program eredménye, de láthatóvá válik az is, hogy a felállított programtérképen hol tart a program, a jó, a kijelölt irányban halad-e. Az alábbi ábrán egy minta látható az információbiztonsági menedzsment systemcontroll folyamatára,amely jól használható a biztonsági program térképének megtervezéséhez is. Az információbiztonsági programterv szempontjából vizsgálva akkor hatékony program, ha értéket teremt, összhangban van a szervezeti célokkal, beépül az életciklusokba, beépül a változáskezelésbe (vagy a változáskezelés épül be a folyamatokba), a kockázatok értékeléséhez és csökkentéséhez szükséges eljárások a napi rutin részei, de talán szabatosabb az a megfogalmazás, hogy az elfogadott, támogatott folyamatok részévé válnak.
Az 4. ábrán az információbiztonsági irányításra, a rendszerfolyamatok ellenőrzésére láthatunk egy áttekintő mintát. Ez a minta jól alkalmazható egy általános szervezetre olyan vonalvezetőként, amely koncepcionális rálátást biztosít a teendőkre, de ebből fakadóan lehetnek a munkaszervezet függvényében súlyponti eltérések.



4. ábra: Információs biztonsági menedzsment rendszer ellenőrző folyamat, ISACA, CISM Review Manual 2013, Chapter 3, page 155, Information Security Program Development and Management

5. Belső és külső források követelményeinek azonosítása, megszerzése, kezelése és meghatározása.

Mottó: „Amit nem tudunk mérni, azt nem is ismerjük igazán.” [39]

5.1. Értelmezés

Az információbiztonsági vezető sikeressége érdekében birtokában kell, hogy legyen azon tudásnak, amely magában foglalja az információbiztonsági folyamatok irányítását és technikáit. Számos különböző területen, különböző módon és megközelítéssel kell kifejtenie a biztonsági program hatását annak sikeressége érdekében. A biztonsági program megvalósítása során elkerülhetetlenül hatással lesz az üzleti folyamatokra. Széles körű, átfogó illetékesség[40] is szükséges ahhoz, hogy mindezeket a helyzeteket hatékonyan tudja kezelni. A pénzügy, finanszírozás, beszerzés, szerződéskötési eljárások, belső eljárásrendek és a szervezeti humánpolitikára[41] egyaránt rálátása és ráhatása kell, hogy legyen. Együtt kell, hogy tudjon működni mindegyik csoporttal a szabályok átlátása és a kontroll pontok folyamatokba történő beillesztése végett. Ezen kívül olyan személyes kompetencia is szükséges, amelynek révén nem csak az egyes csoportokkal tud jól és hatékonyan együttműködni, hanem arra tudja ösztönözni a munkavállalókat, hogy megszerezzék a szükséges ismereteket az információbiztonsági program sikeres teljesítésének érdekében. Fontos kiemelni, hogy a tréning, oktatási program kidolgozása és elkezdése előtt erősen javasolt a meglévő készségek és képességek lemérése, megfigyelése, annak érdekében, hogy láthatóvá váljon, mely területek fejlesztésére van elsősorban szükség. A program lehetőséget biztosít a kölcsönös információcserére is, hiszen itt visszacsatolások érkeznek a napi munkafolyamatokról is, amely értékes információkkal szolgálhat az információbiztonsági program (esetleges további kontrollpontok beiktatása) és a képzés továbbfejlesztéséhez is. A képzésre a modern technológia számtalan lehetőséget biztosít. Általánosságban igaz viszont, hogy az oktatási program szempontjának kell alárendelni a technikát. Tehát bármennyire is felkapott az e-learning, nem biztos, hogy ez a kizárólagos megoldás. Természetesen ez az oktatás, megértés hatásfokán mérhető leginkább. Az információbiztonsági oktatás

[39]Harrington

[40] A nemzetközi ajánlások alapján az információbiztonsági vezető a felső vezetés tagja és szervezetileg közvetlenül a legfelső vezető alá tartozik.

[41] Az érintett, mérvadó osztályok vezetőit javasolt delegálni az információbiztonsági tanácsba.

kidolgozása alapos megértést követel, a rendelkezésre álló eszközök és technológiák mellett láthatóvá kell, hogy váljon annak korlátai is.

5.2. Alapvető elvárások és koncepciók

Tisztázni kell, hogy miben és hogyan méri a felsővezetés a sikerességet, mikor számít majd a program sikeresnek. A program értéket kell, hogy közvetítsen, amely által jobban, hatékonyabban tudja a munkavállaló ellátni a feladatait. A programban való részvétel, annak jó (vagy kiemelkedően jó) teljesítése akár az előmeneteli lehetőségeihez is hozzájárulhat ezáltal. Ahogy a fentiekben szó volt róla, a szervezet egészére a program implementálása felsővezetői támogatást (sőt példamutatást) is igényel. Ezen kívül fontos tisztázni, hogy a szervezet milyen további erőforrásokat tud rendelkezésre bocsátani. Ez nagyban függhet a program céljaitól, a szervezet méretétől, a munkavállalók számától és földrajzi elhelyezkedésétől is. Milyen személyi feltételek adottak a cégnél, azaz például a program koordinációját, lebonyolítását fel tudja-e vállalni az oktatási csoport. Egyértelműen meg kell fogalmazni és elérhetővé kell tenni a partnerek, beszállítók számára a biztonsági követelményeket és minősítési eljárásokat. Erre a legegyszerűbb példa, a portás vagy biztonsági őr, aki kiszervezett munkavállalóként dolgozik, mégis kritikus fontosságú az általa ellátott feladat. A munkaszervezet szempontjából kritikus, hogy tisztában legyen ne csak a szabályokkal, hanem azzal is, hogy éles helyzetben milyen cselekvési lehetőségei vannak, kihez fordulhat. (Gyakran a portás érzékeli elsőként az incidenseket, illetéktelen belépő, áramszünet, egyéb esemény). A munkaszervezet által alkalmazott technológiákat legalább ismertetés szintjén be kell mutatni a munkavállalóknak. Az előbbiekben felsoroltak mind részét kell, hogy képezzék egy olyan térképnek, amely meghatározza a fejlesztési útvonalat, egyértelművé teszi minden egyes kolléga számára, hogy milyen kötelezettségei, feladatai, felelőssége van az információbiztonsággal összefüggésben. Ide sorolható még a szerződések tartalma is, amely biztonsági kontrollként funkcionál a biztonsági szint fenntartására.[42]Gyakori hiba a program megtervezését követően, hogy hirtelen nagy célok kerülnek kitűzésre, túlságosan rövid határidővel.

[42] A 6.5.2-es rész részletesebben tárgyalja a szerződésekkel kapcsolatos tudnivalókat.

5.3. Áttekintés

Általában véve igaz, hogy a kitűzött célokat kicsit túlvállalják (időben, erőforrásban), viszont a rendelkezésre álló erőforrások a kivitelezés során gyakran olvadásnak indulnak, kevesebb lesz a forrás, gyorsabban halad az idő. A már megfogalmazott első tanács az információbiztonsági program kapcsán az volt, hogy az első intézkedés mindig legyen sikeres, tehát először valamilyen könnyen, nagy biztonsággal és viszonylag rövid időn belül elérhető célt érdemes választani. Ez megadhatja az egész további program alaphangját, erre már lehet építkezni.

Az emberi kapcsolatok fontosságáról szintén volt már szó. Az első sikeres együttműködés, az első sikeres oktatás jó promóciós lehetőség a szervezetben. Minden egyes ilyen személy a program reklámja lehet, amennyiben valóban sikerült értéket átadni.

A források, amelyek általában végesek, gyakran csak a személyes időre és a további munkavállalók által nyújtott kollegiális segítségre épülnek kezdetben. Tehát a támogatás esetleg nélkülözi a nagyobb pénzügyi lehetőségeket. Ne adjuk fel ebben az esetben sem, komoly eredményeket lehet elérni, melyek riportolásával, szűkebb vagy bővebb körben történő bemutatásával előbb – utóbb további forráslehetőségek nyílhatnak meg.

A kockázatok csökkentésére vonatkozó lehetőségek, adott tevékenység elutasítása, kockázatcsökkentése, kiszervezése kapcsán ebben a fejezetben a hangsúly a kiszervezésen lesz, olyan SLA-kat kell készíteni, amelyek abban nyújtanak segítséget a beszállítónak, hogy saját maga is jól lássa, milyen transzparens mérőszámokat kell teljesíteni szállításkor. A szervezetben használt szolgáltatásokat és alkalmazásokat érdemes a képzési programba beépíteni, ismertetni. Azon technikákra is érdemes említés szintjén kitérni, amelyek esetleg csak részben, vagy nincsenek (még) jelen a szervezet szolgáltatáshasználati portfóliójában, vagy az adott osztályon nem, de más osztályokon használják.[43]

5.4. Források, amelyek szükségesek az információbiztonsági program végrehajtásához

Az előbbiekben már áttekintésre került, hogy az információbiztonság a szervezet egészére és minden folyamatára, azon túl pedig a partnerekre, beszállítókra is kiterjed, hatást gyakorol. A források kapcsán megemlítésre került, hogy a stratégia szervezetre implementálása során figyelembe kell venni azokat a tényezőket, hogy milyen erőforrások

[43] Az oktatásnak javasolt a munkahelyen kívüli, de jellemző veszélyforrásokra is kitérnie.

állnak rendelkezésre. Ezek közé soroltuk az időt, emberi erőforrást, különböző osztályokkal történő együttműködést, a technikai és folyamatok által biztosított hátteret is, nem utolsó sorban természetesen a pénzügyi forrásokat is. Mindezeken túl foglalkoztunk azzal is, hogy az előrehaladást bemutató mérőszámok, a kommunikáció nagyban hozzájárulhat a program sikerességéhez.

Tehát be kell tudni mutatni az információbiztonsági program eredményeit. Figyelembe kell venni a technikai erőforrásokat, nem csak azért, mert ez olyan tényező, amit vétek lenne nem kihasználni, de az adott osztállyal történő együttműködés, a szervezeti célok jobb megértése és az ismerős technikák implementálása a programba mind sikertényező lehet. Fel lehet használni, ezáltal számos technikai, alternatív csatornát is a kommunikációra. Sőt nem szükséges, hogy minden üzenet az információbiztonsági vezetőtől, vagy csoporttól induljon el. Az ezen koncepció mentén, tervezetten megvalósuló kommunikáció hozzájárul ahhoz az elváráshoz, hogy mindeni tisztában legyen a feladatával, teendőjével, szerepével és felelősségével, valamint aktuális képességével, felkészültségével is. Az adminisztratív tényezőkről sem szabad elfeledkezni, a kommunikáció megszervezése, a bejelentések fogadása, de a képzést követő elismerő oklevél mind ide sorolható.

Világosan megmutatkozik az koncepció, hogy a stratégia független a technológiai megközelítéstől, amely általános ajánlásként igaz is, azonban a program implementációjában, a szervezetre szabásban már érdemes figyelembe venni. Alapvető elvárás, hogy a biztonsági vezető, a könyvben már részletezett ismereteken kívül, ismerje a szervezeti folyamatokat valamint, hogy az informatikai területeken milyen megvalósítások terjedtek el, a megoldásokat és megoldásszállítókat is ismerje. Az alábbi lista felsorol néhány példát a fontosabb technológiai megoldásokból:

- tűzfalak
- antivírus rendszerek
- beépített biztonsági lehetőségek a hálózati eszközökben (például: router, switch)
- behatolás detektáló rendszerek (IDS, HIDS, NIDS)
- behatolás megelőző rendszerek (IPS)
- titkosítási technológiák (PKI, AES) [44]
- digitális aláírások
- smart kártyák

[44] PKI: Public Key Infrastucture, AES: Advanced EncryptionStandars

- authentikációs megoldások
- vezeték nélküli módszerek
- alkalmazás biztonsági módszerek
- távoli hozzáférést biztosító módszerek
- web biztonsági technikák
- log gyűjtő, elemző és korrelációs megoldások
- sebezhetőség vizsgálat és behatolást tesztelő eszközök
- adatszivárgást megelőző módszerek
- adat integritást biztosító eljárások
- azonosító és hozzáférés menedzsment rendszerek

Az itt felsoroltak jobbára biztonsági technológiákkal kapcsolatosak, bár számos funkció a kontrollal áll összefüggésben, mégis alapvetően a biztonság következményeiben nyújtanak segítséget ezen technikai alkalmazások. További technológiákkal kapcsolatos ismeretek is szükségesek, tágabb aspektusban értelmezve például, de nem kizárólagosan:

- helyi hálózatok (LAN)
- nagyobb kiterjedésű hálózatok (WAN)
- mentési és archiválási technikákkal kapcsolatos ismeretek (RAID, SAN)
- Internet és hálózati protokollok (TCP/IP, UDP)
- operációs rendszerek
- hálózati routing koncepciók és protokollok
    - *adatbázisok, szerverek, nagyvállalati, nagykiszolgálós elosztott architektúrák
    - virtualizációs megoldások
    - felhő alapú megoldások
    - web alapú szolgáltatások és technológiák

A hatékony és szervezetre szabott program kidolgozása érdekében tisztában kell lennie a fenyegetettségekkel és a rájuk adott válaszokkal is ezen technikák felhasználásával, különösen a szervezet által felhasználtak vonatkozásában.

5.4.1. Az információbiztonsági program térképének elkészítése

A legfontosabb célok stratégiai összehangolása, a kockázatkezelés, az értékteremtés, az erőforrás-gazdálkodás, a folyamatok beépülésének biztosítása, kontrollpontok létrehozása és a teljesítmény mérése általánosan definiált kell, hogy legyen egy bizonyos szintig a biztonsági stratégiában. A program fejlesztési folyamata megköveteli a megfogalmazott hat célterületen a részletek tisztázását. Minél inkább sikerül minden területen ennek elérése, úgy tisztulnak le a kulcsfontosságú célok. Ezek akár csak részleges elmaradása is oda vezethet, hogy a vezetők vagy érdekelt felek irreális elvárásokat támasztanak az eredményekkel szemben, vagy olyat, amelyikre nincs jelentős befolyásunk. Ebből könnyen következhetnek rossz eredmények, illetve egész pontosan olyan eredmények, amelyek nem esnek egybe az elvárásokkal. Ennek elkerülése érdekében, világos, egyszerű, kis lépésekre tagolt menetrendet, térképet érdemes kidolgozni. A térkép[45] követése meghatározza a programot, az aktuális állapot – térképen történő ábrázolása – pedig vizuális visszaigazolást ad az elért eredményekről.

Például: Az első fázis lehet, hogy egy alprogramot hozunk létre, amely megmutathatja a program szükségleteit a szervezeti stratégiával való összehangoláshoz. Ennek érdekében az információbiztonsági vezető tiszta lappal indulva megbeszéléseket kezdeményezhet az érintettekkel, mint például a HR, jogi, pénzügyi és további, a szervezet életében jelentős osztályok vezetőivel. Ezen megbeszélések célja közösen áttekinteni és meghatározni a fő szervezeti problémákat és kérdéseket. Az interjúk arra is alkalmasak, hogy az információbiztonsági tanács tagjaira javaslatok szülessenek.

A második fázisban ez a fórum felhasználható arra, hogy a vázlatos (nem végleges, még alakítható) információbiztonsági tervezetet, annak implementálását jóváhagyja a társosztályok felsővezetése, ill. az értékes észrevételek beépülhessenek a programba. Ezt követően információbiztonsági irányító tanáccsal közösen definiálásra kerülnek a biztonság számára reprezentáns üzleti célok, tételesen és felsorolásszerűen.

A harmadik fázisban a tanács tagjai be kell, hogy töltsék funkcionális szerepüket, ezáltal elősegítve a szabályzatok tudatosítását, ráirányítva a figyelmet a szabályzatokra. A belső biztonsági áttekintések vizsgálatával érdekeltekké válnak a megfelelőség elérésében és ezen állapot kommunikálásában is.

[45] Angol irodalomban: securityroadmap.

A negyedik fázisban a megfelelőségi hiányosságok és biztonsági értékelések felhasználhatóak a figyelemfelhívásra, a változtatásra, annak nyomon követésére a megfelelőség elérését célzó stratégia fejlesztése során. Ezekre az alapokra tud építkezni a továbbiakban az információbiztonsági vezető, folytathatja a munkát, immár szélesebb körű ismertetéssel a szerepek és felelősségek, folyamatok és eljárások tekintetében, amelyek a biztonságot hivatottak támogatni.

Napjainkban is számos remek információbiztonsági szabályzat, stratégia található egyes szervezeteknél. Ezek a fentebb leírtaknak sok szempontból megfelelhetnek, magukban foglalják az ellenőrzési és fejlesztési tevékenységeket, célokat. Azonban sok ezek közül mégsem ér el sikereket, nem tölti be a valódi funkcióját. Ezért fontos, hogy a fejlesztés során a felelős fókuszt tudjon váltani, át tudja látni, hogy valóban támogató lesz-e a szabályozás az adott folyamatba beépülve. Fel kell tudnia mérni, hogy ezen új tevékenységek nem lesznek-e zavaróak valamely másik szervezeti tevékenység számára. Felkészült-e a szervezet a változásra, annak mértéke még elfogadható nagyságú. Ilyenkor a kulturális és egyéb tényezőket is figyelembe kell venni. Mindezek alapján látható, hogy a szervezetet folyamatosan érő külső- belső hatások miatt a fejlesztés is állandó folyamat kell, hogy legyen. A biztonsági program térképe is vélhetőleg néha újragondolásra, újratervezésre kerülhet.[46] Azonban fontos, hogy legyenek olyan mérföldkövek, amelyek mint mindenképpen elérendő célok szerepelnek a térképen. Egyes változtatások olykor csak annyiban befolyásolják a térképet, hogy az oda vezető út változik meg, a mérföldkő, az elérendő cél változatlan marad, annak legfeljebb időbeli terve, prioritása változik.

	1. szervezet	2. szervezet	3. szervezet
Jogi és szabályozási követelmények	Az együttműködés jelentős változtatásokat igényel az adatfolyamban	Gyakori helyszíni ellenőrzések szakítják meg a folyamatokat a hosszú távú projektekben	Léteznek korlátozások az adatok megosztására a szolgáltatások szállítójával

[46] A kockázati térképre jelentős hatással van a változáskezelés, a kockázatok értékelése.

Fizikai és környezeti tényezők	A számítógépes terem egy könnyen hozzáférhető szinten, emeleten található komoly árvízkockázattal.	Az adatközpont működtetése ki van szervezve.	Az adatközpont a negyedik emeleten van és megfelelő a környezeti kontroll
Etikai tényezők	Hozzáállás: "Ha én látom a képernyőmön, akkor az az enyém."	Hozzáállás: "Ha én tudom használni, hogy bevételt hozzon, akkor az az enyém."	Hozzáállás: "Ha szükség van rá, akkor az én kérésemet el kell fogadni."
Kulturális és regionális eltérések	A szervezeti kultúra elősegíti az információ megosztását.	Keserves harc előzi meg, néha gátat vet a szabályozó folyamatok jóváhagyásának.	A vezetőség "hangja" támogatja a biztonsági célokat.
Költség	A cég csődközelben van és nem képes költeni az IT-ra	Az összes információbiztonsági projektnek muszáj költség-igazoltnak lennie.	Az információbiztonsági költségvetés elfogadott, jóváhagyott és megfelelő, indokolt.
Személyzet	Korábbi hackerek felbérlése, általuk céges információk megszerzése	Szórványosan végeznek háttér ellenőrzéseket, amely kockázatértékelések emberi erőforrásokon nyugszanak.	A személyzet szűrési folyamatok uniformizáltan hajtják végre.
Logisztika	Az információbiztonsági menedzser egy fióktelepen / alegységben van elhelyezve korlátozott hálózati	Az információbiztonsági vezető a központban található és nincsen hozzáférése az adatközponthoz.	Az információbiztonsági vezető a megfelelő helyen van elhelyezve a központ és az adatközpont között.

	hozzáféréssel		
Erőforrások	Nincs személy vagy berendezés dedikálva a biztonsághoz	Az információbiztonsági menedzser csapatának hiányos, vagy nincsenek technikai, műszaki ismeretei.	Az információbiztonsági menedzser csapatának van IT gyakorlata, tapasztalata és napi szinten hozzáférnek a technológiákhoz.
Képességek, lehetőségek	Csak dokumentáció	Folyamat koordináció	Vezérlés, szabályozás megvalósítása

5. ábra: Az információbiztonsági térkép tervezésének lehetséges korlátai, ISACA, CISM Review Manual 2013, Chapter 3, Information Security Program Development and Management

5.5. Biztonsági követelmények kiszervezett funkciókhoz és szolgáltatásokhoz

Mottó: „A szabály semmit sem ér, ha elhatározás-szerűen viseled, ha komoran és konokul csörömpöl rajtad; a szabály akkor jó, ha érzéseidbe ivódik és finoman, hajlékonyan támogat.”[47]

A tipikus információbiztonsági program az operatív felelősségen kívül számos, a biztonsággal kapcsolatos szolgáltatást is biztosíthat. Természetszerűleg ezen szolgáltatások köre, típusa eltérhet egyes szervezetek vonatkozásában tevékenységeik, szolgáltatásaik függvényében. A harmadik fél által biztosított biztonsági szolgáltatások és a kiszervezett IT vagy üzleti folyamatokat tekintetében egyaránt érvényes, hogy az információbiztonsági

[47] Weöres Sándor

vezetőnek az ezekre vonatkozó szabályokat is integrálnia kell az átfogó információbiztonsági programba.

A legtöbb biztonsági követelmény hasonló, azonban a kritikusság és érzékenység mértékének és tulajdonjogának szempontjából különbségek lehetnek. Például kiszervezett információbiztonsági szolgáltatásnál a folyamat tulajdonosa az információbiztonsági menedzser, míg más kiszervezett szolgáltatásnál a felelősség tipikusan a folyamat tulajdonosé. A harmadik fél által jelentett kockázat a szervezet belső hálózatán jelentős lehet, ezt gondosan mérlegelni szükséges.

A kiszervezés, harmadik fél igénybevételének elsődleges mozgatórugója elsődlegesen gazdasági tényező. Épp ezért nagyon fontos a korai elköteleződés a biztonság mellett annak érdekében, hogy egy ilyen döntés ne csak tisztán gazdasági érvek figyelembevételével történjen, ne történjen indokolatlan kompromisszum a biztonság rovására a költségcsökkentés érdekében. Számos kockázatot figyelembe kell venni, mint a kiszervezés következtében bekövetkező lehetséges eredmény, következmény. Lehetséges példák:

- Alapvető készségek elvesztése
- A biztonsági folyamatok átláthatóságának hiánya
- Új hozzáférések és egyéb kontrollal kapcsolatos kockázatok
- A harmadik fél életképessége (stabilitása)
- Az incidens menedzsment összetettsége
- Kulturális és etikai különbségek
- Nem várt költségek és szolgáltatási hiányosságok

A szállító megfelelőségének kontrolljait nyomon kell követni és a szerződés időtartama alatt biztosítani kell, hogy a biztonság mérése ne kerüljön marginális helyzetbe a költségcsökkentés nyomása alatt. Erre egyik megoldás független audit révén és / vagy helyszíni látogatással valósul meg a szállító telephelyén, a kontrolloknak megfelelően. Az egyik legerősebb kontroll a szabályozásban a jó, pontos, precíz szerződés. A szerződésben foglaltak jelenthetik a legnagyobb biztosítékot a szerződés időtartama alatt a megfelelőség biztosítására.

Figyelembe kell venni, hogy országonként más törvények vonatkozhatnak az adatkezelésre, erre vonatkozóan a 2013. évi L. törvény is fogalmaz meg kötelezettségeket, hogy milyen székhellyel rendelkező szolgáltatók vehetőek igénybe. Míg az IT infrastruktúra

kiszervezése esetén a technikai kontroll alkalmazása nyilvánvalónak tűnhet, addig az üzleti folyamatok megkövetelik, hogy képzéssel, tudatossággal, manuális ellenőrzéssel és monitoringgal (helyszíni ellenőrzéseket is tartva) biztosítani kell, hogy a harmadik fél telephelyein megfelelően kezelik a folyamatokat, a fizikai és elektronikus adatokra vonatkozó sztenderdek betartásra kerülnek.

A kiszervezés jó megoldás lehet, megfelelő körültekintéssel. Egy 2006-os tanulmány[48] szerint a biztonsági rések ötödét külső beszállítók okozzák. Tehát talán túlzásnak tűntek a fenti sorok, amelyek helyszíni ellenőrzésre és személyes bejárásra vonatkoztak, azonban látható, hogy komoly biztonsági kockázat rejlik a megfelelő beszállító kiválasztásában. Az alábbiak figyelembevételét ajánlja általánosságban a szakirodalom:

- Azon erőforrások elkülönítése, amelyekhez a külső partner hozzáfér
- Integritás és megbízhatóság az adatok és tranzakciók vonatkozásában
- Védelem rosszindulatú kód és tartalom ellen
- Titkos és bizalmas megállapodások és eljárások
- Biztonsági sztenderdek a (tranzakciós) rendszerekre
- Adatátvitel titkosítás
- Identitás és hozzáférés menedzsment a külső szállítónál
- Incidens felelős – kontakt személy és eszkalációs eljárások.

5.5.1. Harmadik fél hozzáférése

A szervezet bármilyen erőforrásához, bármilyen körülmények között hozzáférés csak szabályozott kockázatelemzésen alapuló kontrollok mellett lehetséges harmadik félnek. Úgy, hogy a szolgáltatási szintekre vonatkozó megállapodások (SLA-k) egyértelműen definiálva legyenek. A hozzáférési szinteket, magukat a hozzáféréseket úgy kell kialakítani, hogy a „legkevesebb szükséges jogosultság” elve érvényesüljön, mérlegelve, hogy mi az, amit „szükséges tudnia” és mi az, amit „szükséges megtennie”. Fontos figyelembe venni és a kockázatok között beárazni, hogy a külsős beszállítónak más üzleti kultúrája lehet, más etikai normák mentén működik. Az információbiztonsági vezetőnek meg kell győződnie, hogy ami

[48]PGP-Vontu

a saját szervezetében szabályozottan zajlana, az a kiszervezett szervezetnél is úgy történik.[49] Általánosságban véve az információbiztonsági vezetőnek legalább ugyanazokat a tevékenységeket el kell látnia, mintha szervezeten belül lenne az egység, így viszont többletfeladatok is adódnak.
A hozzáférések és a hozzáférési kérések teljesen naplózásra és átnézésre kell, hogy kerüljenek a biztonsági vezető (csapata) által, a szabályozott eljárásoknak megfelelően. Ennek gyakorisága döntés alapú, de figyelembe kell venni, mérlegelni szükséges:

- Kritikus információ, amelyhez hozzáférési jogot kaptak.
- Kritikus kiváltságokat kaptak.
- A periodicitást, amely a szerződésben szerepel.
- A szerződés időtartamát.
- A változás - és kockázat kezelési eljárásra vonatkozó iteratív eljárásra vonatkozó szabályozást.

Valamint bármilyen rendellenességet azonnal jelenteni kell a vagyontárgy tulajdonosának. Itt ez lehet architektúra elem, de akár adat is. Az intézkedést meg kell kezdeni az eszkaláció érdekében. A szerződés megszűnését követően a harmadik fél hozzáféréseit azonnal meg kell szüntetni, késlekedés nélkül. A hálózati és információkhoz történő hozzáférés nem adható ki egészen addig, míg a szerződés ténylegesen alá nincs írva. A szerződésnek tartalmaznia kell a hozzáférési szabályokat, kontroll elvárásokat és azon biztosítékokat, amelyek szerződéses garanciákat biztosítanak a szerződés időtartama alatt.

5.5.2. Szerződések

A kiszervezéssel, szolgáltatás kihelyezéssel (outsourcing) kapcsolatos szerződések alapvető célja a résztvevő felek biztosítása, a felelősségek és jogok tisztázása, a nézeteltérések tisztázásának eszközeire is kitérve. Ennek keretében vannak olyan rendelkezések, amelyek a biztonság és információvédelem szempontjából az információbiztonsági vezetőnek (feladatainak ellátása érdekében) meg kell ismernie. Egy ilyen megállapodásnak lehetnek

[49] Például: jól látható a beszállítónál a biztonsági tevékenység, úgy mint a változáskezelés, sérülékenységek azonosítása, incidensek jelentése és az azokra adott válaszokon keresztül egyértelműen definiáltak a jelentési folyamatok, azok formája és struktúrája.

bizalmas, vagy titoktartási kötelezettségre vonatkozó záradékai is. Minden résztvevőnek egyet kell értenie abban, hogy bármilyen bizalmas vagy érzékeny információt kap a szerződés részeként, azt bizalmasan, megfelelő intézkedésekkel kell kezelni. A szerződésnek ki kell térnie a szerződés megszűnésekor szükséges teendőkre, (például: szabadalmi iratok, bizalmas információk megsemmisítése) mikor kell, hogy megtörténjen az adott intézkedés. Meg kell határozni a megsemmisítés elfogadott metódusát is például: papírok ledarálása, égetés, lemágnesezés, fizikai megsemmisítés. A szerződésben kikötött megfelelő biztonsági intézkedések és ellenőrzések szintjét is részletesen definiálni szükséges. Tehát nem elegendő például azt elfogadni, hogy valamilyen szabványos irányítási vagy biztonsági keretrendszernek[50] megfelel a szerződő fél. Arra is érdemes kitérni, hogy mi biztosítja a védelem hatásosságát, hiszen a keretrendszer önmagában ezt nem képes garantálni. Amennyiben elektronikus kapcsolat épül ki a szerződő felek között, akkor a szerződésnek foglakoznia kell ennek tekintetében is a felelősségi körökkel, akár a technikai követelményeket is definiálni kell. A szerződésben le kell fedni a nem várt, nem tervezett eseteket is. Amennyiben biztonsági incidens történik bármely félnél, meg kell határozni a szerződésben, hogy kinek milyen feladata és felelőssége van, ki vezeti a kivizsgálást, az értesítési eljárásokat definiálni szükséges. Egy aktív incidens folyamán ugyanis nagy a nyomás, felfokozott érzelmi állapotok is lehetnek, így könnyebb ezeket a kérdéseket a szerződésben definiálni előre. Végül a szerződés kell, hogy tartalmazzon kártérítési záradékot, amely kompenzációt biztosít a hatások ellentételezésére. Ki kell térni a szerződő felek szervezeteiben az információkat feldolgozó egységek megfelelő szintű szabályozására. Annak függvényében, hogy az üzleti folyamatoknak és a szervezet működését segítő folyamatoknak van szüksége harmadik fél szolgáltatásaira, a szerződésnek tartalmaznia kell néhány komplex biztonsági kérdést, ki kell terjednie például az alábbiakra.

- A kiszervezett szolgáltatások részletes specifikációja (válaszadási idők, teljesítménytényezők)
- Másolásra és eszközök biztonságára vonatkozó korlátozások
- Hozzáférés tiltása külön engedély hiányában és lista vezetése, karbantartása arról, hogy kiknek van hozzáférése.
- Audithoz, felülvizsgálathoz, ellenőrzéshez való jog
- Kártérítési záradékok, a hatások csökkentése érdekében a szolgáltatást szállító által

[50]Ilyenek például: ISO / IEC 27001, 27002 vagy COBIT.

- Üzletmenet folytonosságra vonatkozó tervek (BCP)
- A szolgáltatások színvonalának meghatározása
- Integritás és bizalmasság az üzleti vagyontárgyak tekintetében (ide értve az információt is)
- Titoktartási megállapodások melyeket minden érintettnek (munkavállalóknak is) alá kell írnia
- Szellemi tulajdon védelme
- A tulajdonjogra vonatkozó információk
- A lényeges jogi és szabályozási követelmények teljesüljenek
- Meg kell bizonyosodni, hogy a szerződés végén visszaszolgáltatás vagy megsemmisítés az információn vagy vagyonelemen teljesül-e
- Definiált legyen, hogy meddig kell a titkosságot fenntartani
- A harmadik fél munkavállaló és ügynökei kötelesek tiszteletben tartani a szervezet biztonsági szabályzatát
- Eszkalációs folyamatok
- Kockázatértékelés

A harmadik fél hozzáférése kockázati tényező a biztonságra nézve, legyen az akár logikai, akár fizikai hozzáférés. Így erre vonatkozólag is el kell végezni a kockázatértékelést. A nem technikai ellenőrzéseket, mint például a jó szerződési feltételek definiálása vagy a rendszeres ellenőrzések megtartása, az általános monitoring egyaránt fontos módja a kockázatkezelésnek.

5.5.3. Dokumentáció

A dokumentáció készítése és karbantartása egy fontos eleme a hatékony információbiztonsági programnak. Ezek köre általában kiterjed az alábbiakra:

- szabályzatok, sztenderdek, eljárások, irányelvek,
- technikai leírások, rajzok az infrastruktúráról, architektúráról, alkalmazások és adatáramlás,
- tudatossági és képzési program dokumentáció,

- kockázatelemzések, ajánlások, kapcsolódó dokumentumok,
- biztonsági rendszer tervezése, biztonsági politikák és karbantartási dokumentáció,
- működési eljárások és munkafolyamatok leírása (általában véve minél dokumentáltabb eljárásrend),
- szervezeti dokumentáció, szervezeti diagramok, a személyzet teljesítmény céljai, RACI modell, egyéb modellek.

Minden egyes dokumentumhoz – mint ahogy folyamhoz is – tulajdonost kell rendelni, aki felelős a dokumentum karbantartásáért, aktualizálásáért, sablonok esetén a működési nyilvántartásért.[51] A változtatási javaslatokat be kell terjeszteni a vezetőségnek és az információbiztonsági tanácsnak is, jóváhagyásra. A tulajdonos felelőssége, hogy a dokumentum hozzáférhetősége megfelelően szabályozott és ellenőrizhető legyen. Az információbiztonsági vezető meg kell, hogy bizonyosodjon róla, hogy a dokumentációs folyamat és infrastruktúra rendelkezésre áll, jól működik, a címzettek, a jóváhagyás, a változtatás, az ellenőrzött terjesztés (nyilvánosságra hozás) és visszavonás tekintetében. Sok esetben erre külön dokumentumkezelési rendszert alkalmaznak, ami ideális[52] helyzet, hiszen ezen dokumentumok életciklusát rögzíti a rendszer, nem szükséges ez a fajta letéti kezelés a biztonsággal kapcsolatos dokumentumok felett.[53] Az érzékeny, működési, műszaki információkat megfelelően védett helyen, esetleges magasabb kontrollal védve kell tárolni. Követni kell a szervezeti sztenderdeket és jelölni kell a titkosított dokumentumokat.[54] A sztenderdeket és eljárásokat, amennyiben a körülmények változnak, változtatni szükséges, de összhangban kell, hogy legyenek a kihirdetett szabályozással, ami általában ritkábban változik. A verziókövetés elengedhetetlen annak érdekében, hogy biztosítva legyen, hogy valamennyi érdekelt fél ugyanabból a releváns forrásból dolgozik, a dokumentum átnézett és jóváhagyott, megbízható, és közzétehető. A dokumentumok karbantartása nagyban segíthető, gyorsítható dokumentumkezelő rendszerrel, amely képes követni a változásokat, értesíteni az érintetteket. Érdemes olyan függőséget kezelni képes rendszer alkalmazni, amely az érintett eljárásokra, dokumentumokra való hivatkozásokat is kezelni képes, továbbá fontos, hogy

[51] Ennek megvalósításához is jól használható a RACI modell, különösen a 4 különféle érdekelt definiálásának érdekében, ami a változáskezelés szempontjából fontos, hogy minden érintett hozzájusson a megfelelő információhoz.
[52] Ideális abban az értelemben, hogy technikával támogatott és jobb lehet, mint ha kézi úton valósulna meg.
[53] Ez tipikusan az az eset, amikor technikai megoldásokkal támogatjuk a humán faktort. Fontos megjegyezni, hogy csupán támogatásról és nem kiváltásról van szó.
[54] Bizonyos dokumentumok (például szerződések, szabadalmi adatok) esetén a dokumentum egyes részei között is eltérő jogosultsági, hozzáférési szinteket kell definiálni.

mindig csak az aktuális verzió legyen elérhető. Ettől jól láthatóan különüljön el a dokumentum élete, előzményei.[55]

5.6. Informatikai folyamatok irányítása

Az informatikai rendszerek üzemeltetésére és fejlesztésre szolgáló módszertan illetve szabvány és ajánlás gyűjtemény, angol nevén Information Technology Infrastructure Library (ITIL) hatékony támogatást biztosíthat bármely szervezetnek, elsősorban olyanoknak, amelyek informatikai eszközöket, erőforrásokat használnak, ezen keresztül az információbiztonsági vezetőnek is hatékony segítség lehet. Azon szervezetekben ahol ilyen bevezetésre került, folyamatokban kezdtek el gondolkodni, amely jótékony hatását az informatikai részlegen kívül is kifejtheti. Ahol pedig stabil alapokon nyugszik a sztenderdek, eljárások szerinti folyamatmenedzsment, ott sokkal könnyebb dolga van, akár az információbiztonságban érdekelteknek is. Sőt, ennél kicsit tovább menve az állítható, hogy ilyen módszertan[56] nélkül sokkal nehezebb az üzemeltetési kérdések biztonságpolitikai kezelése.

Például vegyük az incidens bejelentést! A fentiekben jól látható módon arra törekszünk, hogy bármilyen eltérést, incidenst észlel a felhasználó, akkor azt jelentse be a megfelelő formában, majd lehetőség szerint pozitív visszacsatolást alkalmazzunk ezt követően. Az ITIL abban segít, hogy garantált legyen minden folyamatnak az életútja, garantált válaszadási idő legyen. A válaszadásra fordított időablak nagysága kiemelten fontos, főleg egy lehetséges incidens-bejelentés esetén. Tehát nem csak az információbiztonsági folyamatokban legyen gazdája, felelőse az adott tevékenységnek, hanem az informatikai üzemeltetésben is köszönjön vissza ez a megközelítés. Ez voltaképpen az információbiztonsági irányítási rendszer informatikai üzemeltetésre vetített transzformációjának is tekinthető abból a szempontból, hogy jól kiegészíti egymást és mindkettő az üzleti folyamatok hatékony támogatását (is) céljának tekinti.

Meg kell említeni, ahogy a biztonság támogatását célzó információbiztonsági folyamatoknál is kiemelésre került, hogy bármely folyamatot tekintünk, azok mögött munkavállalók, emberek állnak. Nem maga a keretrendszer garantálja a folyamatok „jól-definiált” jó

[55] A dokumentum változástörténete fontos információ. Szabályozni szükséges, hogy a változásokat rögzítő információk mennyi ideig, vagy melyik verziószámig legyenek visszakereshetőek.

[56] Az ITIL nem az egyetlen keretrendszer természetesen, az ISO, a COBIT vagy más iparági sztenderdek egyaránt jó alapot biztosíthatnak arra, hogy szabályozottak legyenek egy munkaszervezet eljárásai.

működését, hanem meg kell látni a folyamatok mögött az embert, a szervezeti és üzleti célokat a folyamatok mögött. Ezek összhangja nélkül bármilyen jó keretrendszerről is van szó, ha nem tudjuk megnyerni a szervezeti vezetőket, munkavállalókat, akkor ennek következtében jelentősen csökkenhet az esély a hatékonyságra, a sikerre.[57] Visszatérve az incidens-bejelentésre, ha egy Alfa munkaszervezetben ITIL és COBIT is bevezetésre kerül, de a munkavállalók úgy érzik, hogy ezen folyamatok nem teremtenek értéket, akkor kérdéses, hogy jelentik-e az apró eltéréseket. Hiszen, ha nem tartja fontosnak, nem tartja figyelme fókuszában a tudatossági képzésen hallottakat, a szervezeti kultúra, a munkatársak hozzáállása nem támogató, akkor valóban könnyen elkerülheti akaratlanul is a figyelmét egy kibontakozóban lévő, eszkalálódó esemény.[58]

Ebben a részben áttekintésre kerültek, hogy milyen külső és belső forrásokat lehet jellemzően igénybe venni a biztonsági program végrehajtásához, annak támogatásához. A munkaszervezeten belül a vezetőségtől megszerzett támogatás kell, hogy alapját képezze a programkidolgozásnak. Ezt követően a rendelkezésre álló források tekintetében lehetnek eltérések a kivitelezés módjában és ütemezésében. A jelentős társosztályok vezetőit a biztonsági tanácsba delegálva kialakításra kerülhet a szervezeti támogatás, amely révén az egyes munkavállalók felé is kommunikálni lehet a biztonsági stratégiát.

A modern munkaszervezetekben lehetnek komplex, szerteágazó, nagy szaktudást igénylő folyamatok. Ezeket nem minden esetben lehet, vagy nem minden esetben gazdaságos belső szakemberrel végeztetni. Egyes speciális feladatokat üzleti döntés és kockázatértékelést követően gyakran valamilyen beszállító, harmadik fél végzi. Ennek lehetséges előnyei:

- pénzügyi, gazdasági előnyök,
- speciális területen nagyon magas szintű szaktudás,
- a kockázatok részleges áthárítása,
- szerződéses garanciák és biztosítékok.

Azonban minden egyes szerződést, beszállítót, külső és belső folyamatot egyaránt fel kell tárni, dokumentálni és kockázati szempontból értékelni kell. A kockázatértékelési jegyzőkönyveket, a döntések, megbeszélések, egyeztetésekről készült dokumentumokat is tárolni szükséges, hogy visszakereshetőek legyenek. Azokat a folyamatokhoz meghatározott

[57] A hatékonyságot a munkavállalói teljesítmény szempontjából vizsgálvaazt kell érteni alatta, hogy a dolgozók munkájukat szívvel – lélekkel végzik a szervezeti szabályzatok figyelembevételével.

[58] Maga a keretrendszer nem képes önmagában garantálni a mintaszerű működést.

kapcsolatokat is meg kell vizsgálni, amelyek érintik a többi folyamatot. Ezen túl a folyamatokban érintett személyeknek[59] kötelességük, hogy az esetleges változásokat dokumentálják, arról a megfelelő felületen és folyamaton keresztül tájékoztassák az illetékest, illetékeseket Ez a változáskezelés és kockázatkezelés része kell, hogy legyen minden folyamatnak.

5.7. Zárszó helyett

A biztonság támogatása többféle lehetséges nézőpontból került megközelítésre. Az alábbiakban olyan gondolatokat kerülnek összefoglalásra, amelyek annyira fontosnak tekinthetőek, hogy így a végén kicsit sarkosan, leegyszerűsítve, akár újra szerepeljenek.

Az elfogadható biztonsági szint soha nem nulla, ez következik abból, hogy tökéletesen biztonságos rendszer nem létezik. Az elfogadható biztonsági szintet minden esetben a szervezet vezetése, a menedzsment kell, hogy meghatározza, az információbiztonsági vezető által előkészített jelentés[60] alapján. Élesen külön kell tudni választani a fejünkben az információt[61], mint az adat reprezentálódását és annak fizikai megjelenését, az adathordozót. A biztonsági programban információs és adatkörök számára definiálunk első sorban védelmet, és csak második sorban vesszük figyelembe ennek fizikai reprezentálódását. Mindig szem előtt kell tartani az arányosságot. Azaz olyan védelmi mechanizmusok kidolgozására van szükség, amelyek egyrészt kivitelezhetőek, másrészt olcsóbbak, mint eseményvezérelt helyzetben a teljes helyreállítás költsége.[62] Minden folyamatnak végső soron a szervezeti célokat kell szolgálnia, ennek függvényében kell, hogy megállapításra kerüljön a fentiekben megfogalmazott elfogadható kockázati szint is, és kidolgozásra kell, hogy kerüljön az ennek elérését támogató biztonsági program.

---

[60] Ez a jelentés optimális esetben többféle szcenáriót tartalmaz, levezetve egyes esetekre vetített költségeket, kockázatokat, előnyök és hátrányok figyelembevételével. Ez alapján tud az információbiztonsági vezető javaslatot tenni valamelyik módozat elfogadására.

[61] Az információ megjelenési formáit érdemes az adott munkaszervezetre jellemző példákkal illusztrálni, például: fax, nyomtatott papír, kukába dobott iratok, pen-drive, képernyőről, íróasztalon hagyott iratokról leleshető adatok, információk.

[62] A számítás tennél összetettebb is lehet, hiszen az online reputáció, stb. károkat is be kell árazni.

A kockázatelemzés, sérülékenység elemzés, úgy általában a veszélyeknek az elemzése periodikusan[63] kell, hogy ismétlődjön. Gyakran merül fel a kérdés, hogy mikor kell újra kockázatelemzést végrehajtani. Általánosságban javasolt:

- a kijelölt idő elteltét követően, a szabályzatban meghatározottaknak megfelelően (periodicitás),
- új vagyonelem (hardver, szoftver, adat) keletkezett, került beszerzésre,
- volt a szervezetben nagyobb incidens, hiszen ezen esemény tanulságainak be kell épülnie a kockázatelemzésbe,
- változáskezelés részeként, ha valamilyen kapcsolódó folyamatban változás történt.

Munkaszervezetenként eltérő szabályzatok, eljárásrendek, kontrollok kerülnek alkalmazásra. Ezek elnevezése is változhat szervezetenként. Felmerül a kérdés, hogy akkor mit nevezünk biztonsági kontrollnak. Általában véve minden olyan tevékenység kontrollnak tekinthető, ami minden lehetséges kárt okozó tevékenység megakadályozását, elkerülését, vagy a káresemény bekövetkeztének hatását hivatott csökkenteni. A kontrollok jellemző típusai:

- adminisztratív, azaz szabályozás jellegű kontroll (belső eljárásrend, utasítás, törvény),
- logikai (műszaki vagy technikai) kontroll: szoftverek, hardverek, beléptető rendszer, token, stb.,
- klasszikus fizikai kontroll: kerítés, portás, szögesdrót, fizikai beléptetés, őrkutya, vizesárok.

Ezen kontroll szempontok alapján javasolt legalább két szempontból vizsgálatot végezni: megfelelőség és hatékonyság. Tehát megfelelő-e a kontroll, tényleg arra hat-e (arra a veszélyre) amire ki lett találva. Hatékonyság tekintetében: valóban csökken-e valamilyen (nem kívánt) esemény valószínűsége, hiszen csak abban az esetben tekinthető hatékonynak, ha ez a valószínűség csökken.
Az információbiztonsági kockázatmenedzsment is jelentős fejlődésen ment és megy keresztül. A hagyományos értékelés és elemzés az adatok számszerűsítésére helyezte a hangsúlyt. A kockázatcsökkentés keretében pedig valamilyen gazdaságilag tervezhető és

[63]Egyik jól használható modell a PDCA.

elfogadható szinten próbálja meg tartani a szervezet biztonsági étvágyának megfelelően a kockázatokat.

6. Összefoglalás

Ebben az elektronikus információbiztonsági vezető szakirányú továbbképzési segédletben az információbiztonság egy igen vékony, de fajsúlyos szelete került bemutatásra.[64] Ahogy a tantárgyi megfogalmazásban is szerepel, ez egy információbiztonságra koncentráló menedzserképzés. Az információ számtalan módon reprezentálódik modern környezetünkben, komoly kihívás az ezzel kapcsolatos szabályozás. A terület fő kihívása, hogy ezen szabályozni, védeni szándékozott információhalmazból kíván a szervezet szinte minden munkatársa dolgozni. A munkájához szükséges információ akkor képez értéket, ha a megfelelő információ, a megfelelő időben és az elvárt tartalommal áll rendelkezésre. Ennek azonban további biztonsági vonzatai vannak, a bizalmasság, a sértetlenség és a rendelkezésre állás. További kihívás, hogy az üzleti, szervezeti célok támogatása, értékteremtés úgy kell, hogy megvalósuljon, hogy ezen információkat, annak legkülönfélébb reprezentálódásait eljárásokkal védeni szándékozzuk. Ezen keretrendszerek és a tananyagban leírt eljárások és példák, jó kiindulási ötlettel szolgálnak, segítséget adhatnak akkor is, amikor egy-egy kidolgozott kockázatkezelési javaslat nem kerül azonnal elfogadásra

A szervezeti támogatás megszerzése, amíg az információbiztonság, a megfelelő viselkedés beépül a gondolkodásmódba, a hétköznapokba, hosszú folyamat. Azonban kis eredményeket, célokat akár pár hónap alatt is el lehet érni. Általános javaslat, hogy minél kisebb célt érdemes kitűzni elsőre, viszont annál hangosabb kommunikációja legyen a sikerének. A könyvben hangsúlyosan megjelentek azok a készségek és képességek, amelyek szükségesek a hatékonysághoz, az előbb is említett kommunikáció, általános informatikai és üzletmenetet támogató technikai ismeretek, stb. Javasolt mindig az embert szem előtt tartani, akinek meg kell tudnunk mutatni a hozzáadott értéket, ezen keresztül tudjuk támogatni a szervezeti célokat és betölteni az információbiztonságért felelős vezetői szerepkört. A kommunikációs stratégiát mindig javasolt az adott célcsoportra szabni. Tehát a board meetingen rövid, látványos, diagramokkal és alternatív megoldások illusztrált kockázatértékelés állja meg jobban a helyét, míg a felhasználóknak szóló tudatossági képzésen egy lazább, történetekkel aláfestett oktatás várhatólag jobban emészthető lesz. A tudatossági képzésen a történetek és megtörtén esetek fognak jobban megragadni a résztvevők

[64]Elektronikus információbiztonsági vezető szakirányú továbbképzési szak, http://vtki.uni-nke.hu/szakiranyu-tovabbkepzes/projektbol-fejlesztett-szakiranyu-tovabbkepzesi-szakok/elektronikus-informaciobiztonsagi-vezeto-szakiranyu-tovabbkepzesi-szak

fejében, minden további osztállyal és érintettel ugyan így meg kell találni a közös hangot a sikeres biztonsági program támogatása, végrehajtása érdekében.

7. Felhasznált irodalom

- CISM Review Manual 2014, ISACA (2013)
- Informatikai projektek vezetése, Görög Mihály, Ternyik László. – Budapest: Kossuth K., 2001. – ISBN 963 09 4227 5
- Tipton, Harold F., and Micki Krause, Information Security Management Handbook, Sixth Edition, Volume 1. Auerbach Publications. 2007. Books24x7. http://common.books24x7.com/toc.aspx?bookid=26438
- Peltier, Thomas R..Howto Complete a Risk Assessmentin 5 Daysor Less. Auerbach Publications. 2009. Books24x7. http://common.books24x7.com/toc.aspx?bookid=30507
- Nemzeti Infokommunikációs Stratégia 2014-2020
- ISACA, COBIT 5, Enabling processes chapter
- Illéssy Miklós – Nemeslaki András – Som Zoltán, Elektronikus információbiztonság-tudatosság a magyar közigazgatásban, Információs Társadalom, ISSN 1587-8694, ÁROP 2.2.17 Új közszolgálati életpálya kutatás alapján

8. Ábrajegyzék

Nemzeti Fejlesztési Ügynökség
www.ujszechenyiterv.gov.hu
06 40 638 638

MAGYARORSZÁG MEGÚJUL

A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.